NetIQ® AppManager® for Network Devices

Management Guide

March 2015

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2015 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Contents

About this Book and the Library **5**
About NetIQ Corporation **7**

1 Introducing AppManager for Network Devices **9**

1.1 Brief Overview . . . 9
1.2 Features and Benefits . . . 9
1.3 Proxy Architecture . . . 10
1.4 Scalability Considerations . . . 10
1.5 Counting AppManager Licenses . . . 10
1.6 Reviewing Supported Devices . . . 10

2 Installing and Configuring AppManager for Network Devices **13**

2.1 System Requirements . . . 13
2.2 Prerequisites . . . 13
2.3 Installing the Module . . . 14
2.4 Deploying the Module with Control Center . . . 15
2.5 Silently Installing the Module . . . 16
2.6 Configuring SNMP Permissions . . . 17
2.7 Discovering Network Devices . . . 19
2.8 Upgrading Knowledge Script Jobs . . . 22

3 NetworkDevice Knowledge Scripts **25**

3.1 ATMLink_QoS . . . 27
3.2 ATMLink_Util . . . 30
3.3 Chassis_Usage . . . 32
3.4 Device_Ping . . . 36
3.5 Device_Syslog . . . 37
3.6 Device_Uptime . . . 39
3.7 FrameRelayLink_QoS . . . 41
3.8 FrameRelayLink_Util . . . 43
3.9 FXOPort_Health . . . 46
3.10 FXOPort_Util . . . 47
3.11 FXSPort_Health . . . 48
3.12 FXSPort_Util . . . 49
3.13 Host_CPULoaded . . . 50
3.14 Host_DeviceStatus . . . 52
3.15 Host_MemoryUsage . . . 53
3.16 Host_ProcessDown . . . 54
3.17 Host_ProcessUp . . . 56
3.18 Host_StorageUsage . . . 58
3.19 Interface_Health . . . 59
3.20 IPSubsystem_Util . . . 62
3.21 ISDNChannel_CallVolume . . . 63
3.22 ISDNChannel_Health . . . 65
3.23 ISDNChannel_Util . . . 67

3.24 LANLink_QoS 68
3.25 LANLink_Util 71
3.26 Report_DeviceAvailability 74
3.27 Report_ChassisUsage 75
3.28 Report_ISDNCallVolume 77
3.29 Report_ISDNTimeDetail 79
3.30 Report_ISDNUtilization 80
3.31 Report_LinkUtilization 82
3.32 Report_QoSUtilization 83
3.33 Report_QoSVolume 85
3.34 Report_TotalVolume 87
3.35 SingleATMLink_Util 89
3.36 SingleFrameRelayLink_Util 91
3.37 SingleInterface_Health 93
3.38 SingleLANLink_Util 95
3.39 SingleWANLink_Util 97
3.40 SNMPTrap_AddMIB 99
3.41 SNMPTrap_Async 101
3.42 WANLink_QoS 106
3.43 WANLink_Util 109
3.44 Recommended Knowledge Scripts 112

About this Book and the Library

The NetIQ AppManager product (AppManager) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and health for a broad spectrum of operating environments, applications, services, and server hardware.

AppManager provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager, administrative staff can monitor computer and application resources, check for potential problems, initiate responsive actions, automate routine tasks, and gather performance data for real-time and historical reporting and analysis.

Intended Audience

This guide provides information for individuals responsible for installing an AppManager module and monitoring specific applications with AppManager.

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

Provides complete information about AppManager pre-installation requirements and step-by-step installation procedures for all AppManager components.

User Guide for AppManager Control Center

Provides complete information about managing groups of computers, including running jobs, responding to events, creating reports, and working with Control Center. A separate guide is available for the AppManager Operator Console.

Administrator Guide for AppManager

Provides information about maintaining an AppManager management site, managing security, using scripts to handle AppManager tasks, and leveraging advanced configuration options.

Upgrade and Migration Guide for AppManager

Provides complete information about how to upgrade from a previous version of AppManager.

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

The AppManager library is available in Adobe Acrobat (PDF) format from the AppManager Documentation page of the NetIQ Web site.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Introducing AppManager for Network Devices

This chapter introduces AppManager for Network Devices, providing a brief overview of the module and describing its features and benefits.

1.1 Brief Overview

AppManager for Network Devices monitors a wide array of devices, such as switches, routers, and gateways, by using SNMP to poll Management Information Bases (MIBs).

AppManager is designed to help you gain easy access to network device data, and to help you analyze and manage that data. The AppManager for Network Devices solution minimizes the cost of maintaining network devices, aids in capacity planning, and can prevent downtime.

AppManager for Network Devices includes Knowledge Scripts for creating jobs that monitor the health, availability, and performance of key devices. These scripts allow you to monitor and manage crucial device properties at a depth unparalleled by any other solution. You can configure each Knowledge Script to raise an event, collect data for reporting, and perform automated problem management when an event occurs.

1.2 Features and Benefits

The following are just a few of the features and benefits of monitoring network devices with AppManager:

- Reduces the time that you spend diagnosing and resolving issues
- Monitors chassis resources, including CPU, memory, flash memory, backplane, power supplies, fans, temperature sensors, and voltage sensors
- Monitors the IP subsystem (all packets flowing through a device) for traffic levels and percentage of packet errors
- Monitors physical interfaces for bandwidth usage, packet loss and packet errors, and changes in operational status
- Monitors LAN/WAN links from a logical perspective, link usage instead of interface usage, for changes in operational status, bandwidth, usage, and packet loss/errors
- Accesses the Host Resource MIB, on devices for which it is implemented, to monitor CPU usage, disk and memory storage usage, process CPU, process memory, process status, and device status
- Automates system management issues that could affect network device performance
- Pinpoints problems wherever they originate
- Provides Knowledge Scripts for day-to-day and diagnostic monitoring
- Supports SNMP versions 1, 2, and 3
- Checks for SNMP traps forwarded from NetIQ SNMP Trap Receiver

1.3 Proxy Architecture

You do not need to install the module on every device that you want to monitor. Instead, install the AppManager for Network Devices module on a proxy agent computer. When you run a Knowledge Script job, the module runs on the proxy agent computer and sends messages to and from the devices you are monitoring, using the SNMP `GET` command.

In order for the proxy architecture to function, SNMP must be enabled on the proxy agent computer *and* on the network devices that you want to monitor.

Before you run the Device_Syslog script, configure your network devices to send Syslog messages to the Network Device proxy agent computer.

1.4 Scalability Considerations

Consider the following when installing the module and running the NetworkDevice category of Knowledge Scripts:

- Only one computer should act as a proxy for any given network device.
- One computer should be the proxy for no more than 50 network devices.
- If the proxy agent computer is the AppManager server, limit the associated network devices to ten.
- You should not run NetworkDevice Knowledge Scripts more frequently than the default setting shown on the Schedule tab. The default schedule takes into consideration the fact that monitoring network devices can be a CPU- and memory-intensive process. To run the scripts more frequently than the default schedule is to subject the managed client computer to undue stress.
- You should limit the number of target objects for any given NetworkDevice Knowledge Script job. If you run a script on too many targets, the job will not run correctly. For instance, running the Interface_Health script on multiple routers may seem inconsequential, but some routers can have 200 interfaces or more. Running a job that large will test the limits of your system's CPU and memory resources. In such a situation, AppManager puts the job into Error state, raising an event that advises you to break your job up into smaller pieces.

1.5 Counting AppManager Licenses

AppManager for Network Devices consumes one AppManager license per discovered network device.

1.6 Reviewing Supported Devices

AppManager cannot monitor every conceivable router or switch on a given network. It does, however, discover and monitor limited functions for routers and switches that support MIB-2, such as link usage and interface status. In addition, AppManager can collect information above and beyond the basic MIB-2 information (such as CPU, memory, backplane, fans, voltage, and temperature) for the following devices:

Vendor	Device	Notes
Switches		

Vendor	Device	Notes
Alcatel®	OmniSwitch (6600, 7000, and 8800 series)	
	OmniStack (6100 series)	
Cisco®	All known switches are supported.	
Extreme Networks®	Any switch that supports ExtremeWare v6.1.x and later	
Nortel™	Baystack, 460 Series and later	
Routers		
Alcatel	OmniSwitch/Router series OmniAccess (408 and 512)	
Cisco	All known routers are supported.	
Nortel	Access Stack Node (ASN) Series	BayRS versions 14.x and 15.x
	Backbone Concentrator Node (BCN) Series	Other OS versions are also supported, but not all metrics can be collected.
	Backbone Link Node (BLN) Series	
	Backbone Node (BN) Series	
	Passport Series (including 8600 product line)	
	Passport Advanced Remote Node (ARN) Series	

2 Installing and Configuring AppManager for Network Devices

This chapter provides installation instructions and describes system requirements for AppManager for Network Devices.

This chapter assumes you have AppManager installed. For more information about installing AppManager or about AppManager system requirements, see the *Installation Guide for AppManager*, which is available on the AppManager Documentation page.

2.1 System Requirements

For the latest information about supported software versions and the availability of module updates, visit the AppManager Supported Products page. Unless noted otherwise, this module supports all updates, hotfixes, and service packs for the releases listed below.

AppManager for Network Devices has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computers, on all proxy agent computers, and on all console computers	7.0 or later Support for Windows Server 2008 on AppManager 7.x requires AppManager Windows Agent hotfix 71704 or later. For more information, see the AppManager Suite Hotfixes Web page.
Microsoft Windows operating system installed on the proxy agent computer	One of the following: ◆ Windows 7 (32-bit and 64-bit) ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit and 64-bit) ◆ Windows Server 2003 R2 (32-bit and 64-bit)
AppManager for Microsoft Windows module installed on repository, on all proxy agent, and on all console computers	7.6.170.0 or later. For more information, see the AppManager Module Upgrades & Trials page.

2.2 Prerequisites

Installing the module automatically installs NetIQ SNMP Trap Receiver. For more information, see “Working with NetIQ SNMP Trap Receiver” on page 104.

Do not install the module on any Cisco servers such as CallManager or Unity. Install the module on its own computer, although it is fine to also install modules such as AppManager for VoIP Quality and AppManager for Phone Quality on that computer.

If your repository and management server are on different computers, install the AppManager for Network Devices module on the management server.

2.3 Installing the Module

Run the module installer on all the proxy agent computers (agents) to install the agent components, and run the module installer on all console computers to install the Help and console extensions.

Access the `AM70-NetworkDevice-7.x.x.0.msi` module installer from the `AM70_NetworkDevice_7.x.x.0` self-extracting installation package on the AppManager Module Upgrades & Trials page.

For Windows environments where User Account Control (UAC) is enabled, install the module using an account with administrative privileges. Use one of the following methods:

- Log in to the server using the account named Administrator. Then, run the module installer `.msi` file from a command prompt or by double-clicking it.
- Log in to the server as a user with administrative privileges and run the module installer `.msi` file as an administrator from a command prompt. To open a command-prompt window at the administrative level, right-click a command-prompt icon or a Windows menu item and select **Run as administrator**.

You can install the Knowledge Scripts and the Analysis Center reports into local or remote AppManager repositories (QDBs). The module installer installs Knowledge Scripts for each module directly into the QDB instead of installing the scripts in the `\AppManager\qdb\kp` folder as in previous releases of AppManager.

You can install the module manually, or you can use Control Center to deploy the module to a remote computer where an agent is installed. For more information, see “Checking In the Installation Package” on page 16. However, if you use Control Center to deploy the module, Control Center only installs the *agent* components of the module. The module installer installs the QDB and console components as well as the agent components on the agent computer.

To install the module manually:

1. Double-click the module installer `.msi` file.
2. Accept the license agreement.
3. Review the results of the pre-installation check. You can expect one of the following three scenarios:
   - **No AppManager agent is present:** In this scenario, the pre-installation check fails, and the installer does not install agent components.
   - **An AppManager agent is present, but some other prerequisite fails:** In this scenario, the default is to not install agent components because of one or more missing prerequisites. However, you can override the default by selecting **Install agent component locally**. A missing application server for this particular module often causes this scenario. For example, installing the AppManager for Microsoft SharePoint module requires the presence of a Microsoft SharePoint server on the selected computer.
   - **All prerequisites are met:** In this scenario, the installer installs the agent components.

4 To install the Knowledge Scripts into the QDB:

   4a Select **Install Knowledge Scripts** to install the repository components, including the Knowledge Scripts, object types, and SQL stored procedures.

   4b Specify the SQL Server name of the server hosting the QDB, as well as the case-sensitive QDB name.

   Note Microsoft .NET Framework 3.5 is required on the computer where you run the installation program for the QDB portion of the module. For computers running more recent versions of Windows operating systems that use a newer version of .NET, install .NET 3.5 with the Add Roles and Features wizard in Windows Server Manager, as described in this Microsoft article.

5 (Conditional) If you use Control Center 7.x, run the module installer for each QDB attached to Control Center.

6 (Conditional) If you use Control Center 8.x, run the module installer only for the primary QDB. Control Center automatically replicates this module to secondary QDBs.

7 Run the module installer on all console computers to install the Help and console extensions.

8 Run the module installer on all proxy agent computers to install the agent components.

9 Configure AppManager Security Manager to identify the version of SNMP in use on your network devices. For more information, see Section 2.6, “Configuring SNMP Permissions,” on page 17.

10 (Conditional) If you have not discovered network devices, run the Discovery_NetworkDevice Knowledge Script on all proxy agent computers where you installed the module. For more information, see Section 2.7, “Discovering Network Devices,” on page 19.

11 To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.8, “Upgrading Knowledge Script Jobs,” on page 22.

After the installation has completed, the `NetworkDevice_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\`*`ServerName`* folder, lists any problems that occurred.

2.4 Deploying the Module with Control Center

You can use Control Center to deploy the module to a remote computer where an agent is installed. This topic briefly describes the steps involved in deploying a module and provides instructions for checking in the module installation package. For more information, see the *Control Center User Guide for AppManager*, which is available on the AppManager Documentation page.

Deployment Overview

This section describes the tasks required to deploy the module on an agent computer.

To deploy the module on an agent computer:

1 Verify the default deployment credentials.

2 Check in an installation package. For more information, see “Checking In the Installation Package” on page 16.

3 Configure an email address to receive notification of a deployment.

4 Create a deployment rule or modify an out-of-the-box deployment rule.

5 Approve the deployment task.

6 View the results.

Checking In the Installation Package

You must check in the installation package, `AM70-NetworkDevice-7.x.x.0.xml`, before you can deploy the module on an agent computer.

To check in a module installation package:

1. Log in to Control Center using an account that is a member of a user group with deployment permissions.
2. Navigate to the **Deployment** tab (for AppManager 8.x) or **Administration** tab (for AppManager 7.x).
3. In the Deployment folder, select **Packages**.
4. On the Tasks pane, click **Check in Deployment Packages** (for AppManager 8.x) or **Check in Packages** (for AppManager 7.x).
5. Navigate to the folder where you saved `AM70-NetworkDevice-7.x.x.0.xml` and select the file.
6. Click **Open**. The Deployment Package Check in Status dialog box displays the status of the package check in.
7. To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.8, “Upgrading Knowledge Script Jobs,” on page 22.

2.5 Silently Installing the Module

To silently (without user intervention) install a module using the default settings, run the following command from the folder in which you saved the module installer:

```
msiexec.exe /i "AM70-NetworkDevice-7.x.x.0.msi" /qn
```

where *x.x* is the actual version number of the module installer.

To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.8, “Upgrading Knowledge Script Jobs,” on page 22.

To create a log file that describes the operations of the module installer, add the following flag to the command noted above:

```
/L* "AM70-NetworkDevice-7.x.x.0.msi.log"
```

The log file is created in the folder in which you saved the module installer.

NOTE: To perform a silent install on an AppManager agent running Windows Server 2008 R2 or Windows Server 2012, open a command prompt at the administrative level and select **Run as administrator** before you run the silent install command listed above.

To silently install the module to a remote AppManager repository, you can use Windows authentication or SQL authentication.

Windows authentication:

```
AM70-NetworkDevice-7.x.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_MOINSTALL=0
MO_B_SQLSVR_WINAUTH=1 MO_SQLSVR_NAME=SQLServerName MO_QDBNAME=AM-RepositoryName
```

SQL authentication:

```
AM70-NetworkDevice-7.x.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_MOINSTALL=0
MO_B_SQLSVR_WINAUTH=0 MO_SQLSVR_USER=SQLLogin MO_SQLSVR_PWD=SQLLoginPassword
MO_SQLSVR_NAME=SQLServerName MO_QDBNAME=AM-RepositoryName
```

2.6 Configuring SNMP Permissions

AppManager uses SNMP queries to access network devices and to enable functionality of NetIQ SNMP Trap Receiver. Before discovering network devices, enter SNMP community string information into AppManager Security Manager.

The type of information you configure varies according to the version of SNMP that is implemented on the network device.

AppManager for Network Devices supports SNMP versions 1, 2, and 3.

If you do not indicate an SNMP version, AppManager attempts to determine the version during the Discovery job. This process can be time consuming.

By configuring SNMP information, you provide AppManager the permission it needs to access the Management Information Bases (MIBs) on SNMP-enabled network devices.

Configuration for SNMP Versions 1 and 2

Configure community string and version information for each network device that is being monitored by each proxy agent computer.

Complete the following fields on the Custom tab in Security Manager:

Field	Type
Label	NetworkDevice
Sub-Label	Indicate whether the community string information will be used for a single device or for all devices. ◆ For a community string for a single device for a proxy agent computer, type <*device name*>. ◆ For a community string for all devices for a proxy agent computer, type `default`.
Value 1	Read-only community string, such as `private` or `public`
Value 3	◆ *If the device supports SNMP v1*, type `v1` or `1` ◆ *if the device supports SNMP v2*, type `v2` or `2` If you do not specify either SNMP version, AppManager attempts to determine the version during the Discovery_NetworkDevice job. This process can be time consuming.
Extended application support	Leave this option unselected

Configuration for SNMP Version 3

AppManager for Network Devices supports the following modes for SNMP v3:

- No authentication; no privacy

- Authentication; no privacy
- Authentication and privacy

In addition, the module supports the following protocols for SNMP v3:

- MD5 (Message-Digest algorithm 5, an authentication protocol)
- SHA (Secure Hash Algorithm, an authentication protocol)
- DES (Data Encryption Standard, encryption protocol)
- AES (Advanced Encryption Standard, an encryption protocol, 128-bit keys only)

Your SNMP v3 implementation may support one or more combinations of mode and protocol. That combination dictates the type of information you configure in AppManager Security Manager: user name (or entity), context name, protocol name, and protocol passwords.

Configure SNMP v3 information for each network device that is being monitored by each proxy agent computer.

Complete the following fields on the Custom tab in Security Manager:

Field	Description
Label	NetworkDevice
Sub-Label	Indicate whether the community string information will be used for a single device or for all devices. ◆ For a community string for a single device for a proxy agent computer, type <*device name*>. ◆ For a community string for all devices for a proxy agent computer, type `default`.
Value 1	SNMP user name, or entity, configured for the device. All SNMP v3 modes require an entry in the **Value 1** field.
Value 2	Name of a context associated with the user name or entity you entered in the **Value 1** field. A context is a collection of SNMP information that is accessible by an entity. If possible, enter a context that provides access to all MIBs for a device. *If the device does not support context*, type an asterisk (*). All SNMP v3 modes require an entry in the **Value 2** field.

Value 3	Combination of protocol and password appropriate for the SNMP v3 mode you implemented.
	◆ For no authentication/no privacy mode, leave the **Value 3** field blank.
	◆ For *authentication/no privacy mode*, type `md5` or `sha` and the password for the protocol, separating each entry with a comma. For example, type the following:
	`md5,abcdef`
	◆ For *authentication/privacy mode*, type `md5` or `sha` and the associated password, and then type `des` and the associated password, separating each entry with a comma. For example, type the following:
	`sha,hijklm,des,nopqrs`

Extended application support	Leave this option unselected.

Configuration for Trap Receiver Functionality

If the Trap Receiver device uses different Read and Trap SNMP permissions (for instance, the Read community string is one value and the Trap community string is another), then an additional entry in AppManager Security Manager is required:

- For the Read permission, use the instructions for your version of SNMP in Section 2.6, "Configuring SNMP Permissions," on page 17 and type `NetworkDevice` in the **Label** field.
- For the Trap permission, use the instructions for your version of SNMP in Section 2.6, "Configuring SNMP Permissions," on page 17 and type `SNMPTrap` in the **Label** field.

When you run the Section 3.41, "SNMPTrap_Async," on page 101 script, AppManager searches for Security Manager **Label** entries in the following order:

- SNMPTrap (first specific, then default permissions)
- NetworkDevice (first specific, then default permissions)
- SNMP (first specific, then default permissions)

2.7 Discovering Network Devices

Use the Discovery_NetworkDevice Knowledge Script to discover network resources, such as routers, switches, and gateways, using SNMP `GET` commands over proxy architecture. Upon successful discovery, the following devices can be monitored:

- Chassis resources: CPU, memory, Flash memory, backplane, power supplies, fans, temperature sensors, and voltage sensors
- IP subsystem
- Interfaces: IP address and queue
- Host Resource
- WAN links, serial links, frame relay links, and ATM links

The Discovery_NetworkDevice script also tracks, displays, and provides various alerts about AppManager for Network Devices services.

The Discovery job also discovers NetIQ SNMP Trap Receiver resources. For more information, see "Working with NetIQ SNMP Trap Receiver" on page 104.

Only one computer should act as a proxy for any given network device. Therefore, run the Discovery_NetworkDevice Knowledge Script on only one Microsoft Windows server at a time.

- Ensure that all devices you want to discover have unique names. AppManager cannot differentiate between two IP addresses that have the same value for the `sysName` object, which is a name for a managed node assigned by an administrator, usually the hostname. When two devices have the same `sysName` object, AppManager assumes the two devices are the same single device. The list of devices you can monitor will be inaccurate if you do not assign unique names to your devices.
- Configure AppManager Security Manager with the community string and version information for each device you want to discover. For more information, see Section 2.6, "Configuring SNMP Permissions," on page 17.

If you delete or add a resource object, or if you make any other kind of change that might affect the monitoring of your resources, run the Discovery_NetworkDevice Knowledge Script again to update your list of resource objects. In addition, if you are running this module on AppManager 8 or later, you can use the delta discovery feature in Control Center to run discovery on a schedule to more quickly detect changes to your environment.

Set the Values tab parameters as necessary:

Parameter	How to Set It
Auto Discovery	
Default gateway router	Specify the IP network address of the gateway (router) to query during discovery. Note Use this parameter if you are uncertain of all the relevant subnets that should be scanned during discovery. If you enter an IP address here, AppManager queries the gateway for its routing tables and then attempts to discover every device in the tables.
Maximum number of hops	Specify the maximum number of hops that you want discovery to make during auto-discovery. The default is 1 hop. Discovery considers the gateway router itself to be the first hop. Therefore, a *Maximum number of hops* setting of 1 means you discover only the networks directly connected to the gateway router, and no other routers.
Walk subnets for layer-2 devices?	Set to **n** to discover all routers (Layer-3 devices) and all Cisco switches (Layer-2 devices), within the number of *Maximum number of hops* you have set, by means of routing tables and Cisco Discovery Protocol (CDP). Set to **y** to also discover all non-Cisco switches and other network devices, within the number of *Maximum number of hops* you have set, by means of a range discovery on all discovered subnets. Caution Set this parameter to **y** only with the understanding that walking the subnets for Layer-2 devices is a time- and resource-intensive undertaking that can have a negative impact on network performance. The default is n.
List of network devices	Provide a list of the network devices you want to discover. You must specify at least one network device. Use a comma to separate the names in the list. For example: `raldbellijm02,raldattixlm` You can enter hostnames, if you use DNS in your environment, or IP addresses. **NOTE:** Before running this script, configure the SNMP permissions for each device that you list in this field into Security Manager. For more information, see Section 2.6, “Configuring SNMP Permissions,” on page 17.

Parameter	How to Set It
List of network device ranges	Provide a list of IP address ranges for the network devices you want to discover. Spaces are invalid in the list. Only numbers, dashes, and commas are allowed. For example: `1.2.3.4-5.6.7.8,10.9.8.7-10.10.10.10` Note Limit the number of IP addresses in each range to no more than 256. To scan more than 256 IP addresses, break a range into multiple ranges, each with no more than 256 IP addresses.
Full path to file with list of network devices	Instead of identifying each network device separately, you can specify the full path to a file on the agent computer that contains a device name on each line of the file. The file must be located on the computer on which you run the Discovery script. **NOTE:** Before running this script, configure the SNMP permissions for each device that you list in this field into Security Manager. For more information, see Section 2.6, "Configuring SNMP Permissions," on page 17.
Discovery Details	
Discover individual … … interfaces? … LAN links? … WAN links? … frame relay links? … ATM links? … FXS ports? … FXO ports? … ISDN channels?	This script automatically discovers interfaces, links, and ports when these parameters are set to **y**. The default is y. Note Set these parameters to **n** for any device you do not want to monitor. By not discovering these resources, you will significantly speed the discovery process and improve the performance of the TreeView.
Trap Receiver Discovery	
Discover Trap Receiver?	Set to **y** to discover NetIQ SNMP Trap Receiver. The default is y.
Trap Receiver IP address	Specify the IP address of the computer on which Trap Receiver is installed. The default is `localhost`.
Trap Receiver TCP port	Specify the TCP port number through which Trap Receiver will communicate with AppManager. The default is port 2735.
Discover IP addresses that belong to the same device?	Set to **y** to discover all IP addresses for a single device. The same device will appear in the TreeView once for each different associated IP address. Set to **n** to discover a device only once, regardless of the number of associated IP addresses. Note that the number of discovered devices directly affects the number of licenses required for the AppManager for Network Devices module. The default is n.

Parameter	How to Set It
Discovery timeout	Specify the number of minutes that the script should attempt discovery before stopping as unsuccessful. The default is 10 minutes. The maximum is 60 minutes.
Raise event when discovery succeeds?	This script always raises an event when discovery fails for any reason. In addition, you can set this parameter to **y** to raise an event when discovery succeeds. The default is n.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.

2.8 Upgrading Knowledge Script Jobs

If you are using AppManager 8.x or later, the module upgrade process now *retains* any changes you might have made to the parameter settings for the Knowledge Scripts in the previous version of this module. Before AppManager 8.x, the module upgrade process *overwrote* any settings you might have made, changing the settings back to the module defaults.

As a result, if this module includes any changes to the default values for any Knowledge Script parameter, the module upgrade process ignores those changes and retains all parameter values that you updated. Unless you review the management guide or the online Help for that Knowledge Script, you will not know about any changes to default parameter values that came with this release.

You can push the changes for updated scripts to running Knowledge Script jobs in one of the following ways:

- Use the AMAdmin_UpgradeJobs Knowledge Script.
- Use the Properties Propagation feature.

Running AMAdmin_UpgradeJobs

The AMAdmin_UpgradeJobs Knowledge Script can push changes to running Knowledge Script jobs. Your AppManager repository (QDB) must be at version 7.0 or later. Upgrading jobs to use the most recent script version allows the jobs to take advantage of the latest script logic while maintaining existing parameter values for the job.

For more information, see the **Help** for the AMAdmin_UpgradeJobs Knowledge Script.

Propagating Knowledge Script Changes

You can propagate script changes to jobs that are running and to Knowledge Script Groups, including recommended Knowledge Script Groups and renamed Knowledge Scripts.

Before propagating script changes, verify that the script parameters are set to your specifications. You might need to appropriately set new parameters for your environment or application.

If you are not using AppManager 8.x or later, customized script parameters might have reverted to default parameters during the installation of the module.

You can choose to propagate only properties (specified in the **Schedule** and **Values** tabs), only the script (which is the logic of the Knowledge Script), or both. Unless you know specifically that changes affect only the script logic, you should propagate the properties and the script.

For more information about propagating Knowledge Script changes, see the “Running Monitoring Jobs” chapter of the *Control Center User Guide for AppManager*.

Propagating Changes to Ad Hoc Jobs or Knowledge Script Groups

You can propagate the properties and the logic (script) of a Knowledge Script to ad hoc jobs started by that Knowledge Script. Corresponding jobs are stopped and restarted with the Knowledge Script changes.

You can also propagate the properties and logic of a Knowledge Script to corresponding Knowledge Script Group members. After you propagate script changes to Knowledge Script Group members, you can propagate the updated Knowledge Script Group members to associated running jobs. Any monitoring jobs started by a Knowledge Script Group member are restarted with the job properties of the Knowledge Script Group member.

To propagate changes to ad hoc Knowledge Script jobs or Knowledge Script Groups:

1. In the Knowledge Script view, select the Knowledge Script or Knowledge Script Group for which you want to propagate changes.
2. Right-click the script or group and select **Properties propagation** > **Ad Hoc Jobs**.
3. Select the components of the Knowledge Script that you want to propagate to associated ad hoc jobs or groups and click **OK**:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, such as schedule, monitoring values, actions, and advanced options. If you are using AppManager 8.x or later, the module upgrade process now *retains* any changes you might have made to the parameter settings for the Knowledge Scripts in the previous version of this module.

3 NetworkDevice Knowledge Scripts

AppManager for Network Devices provides the following Knowledge Scripts for monitoring network devices such as routers, switches, and voice gateways by means of SNMP polling of Management Information Bases (MIBs). Using SNMP GET commands, NetworkDevice scripts monitor the basic subsystems that are common to all devices, such as CPU, memory, and the chassis.

AppManager for Network Devices supports SNMP versions 1, 2, and 3.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ATMLink_QoS	Monitors QoS on ATM links on a Cisco IOS device for traffic class usage, dropped packet rate, and queue depth.
ATMLink_Util	Monitors the usage of the parent resource of the ATM links on a network device.
Chassis_Usage	Monitors the physical chassis of a network device, including CPU, RAM, flash memory, backplane, temperature sensors, voltage sensors, and fan sensors.
Device_Ping	Checks the availability of network devices that respond to ICMP Echo requests.
Device_Syslog	Listens for UDP traffic on port 514.
Device_Uptime	Monitors the number of hours that a network device or its network management component has been operational since its last reboot.
FrameRelayLink_QoS	Monitors QoS on frame relay links on a Cisco IOS device for traffic class usage, dropped packet rate, and queue depth.
FrameRelayLink_Util	Monitors the usage of a parent resource for the frame relay links on a network device.
FXOPort_Health	Monitors signal errors on an FXO port on a network device.
FXOPort_Util	Monitors FXO port usage on a network device.
FXSPort_Health	Monitors signal errors on an FXS port on a network device.
FXSPort_Util	Monitors FXS port usage on a network device.
Host_CPULoaded	Accesses the Host Resource MIB to monitor CPU usage on a device.
Host_DeviceStatus	Accesses the Host Resource MIB to monitor the status and error count for a device.
Host_MemoryUsage	Accesses the Host Resource MIB to monitor memory usage on a device.
Host_ProcessDown	Accesses the Host Resource MIB to determine whether a specified process is not running on a device.

Knowledge Script	What It Does
Host_ProcessUp	Accesses the Host Resource MIB to determine whether a specified process is running on a device.
Host_StorageUsage	Accesses the Host Resource MIB to monitor storage usage on a device.
Interface_Health	Monitors the parent resource for the interfaces on a network device.
IPSubsystem_Util	Monitors the IP subsystem of a network device.
ISDNChannel_CallVolume	Measures the number of incoming calls, the number of outgoing calls, and the percentage of call failures (dropped calls) on a device.
ISDNChannel_Health	Monitors the operational status of ISDN bearer channels and the up-or-down status of signaling channels.
ISDNChannel_Util	Measures the usage of ISDN channels on a device.
LANLink_QoS	Monitors QoS on LAN links on a Cisco IOS device for traffic class usage, dropped packet rate, and queue depth.
LANLink_Util	Monitors the parent resource for the LAN links on a network device.
Report_ChassisUsage	Summarizes the Good-Acceptable-Poor (GAP) and average usage for CPU, memory pool, and backplane for a network device.
Report_DeviceAvailability	Summarizes the availability of selected network devices.
Report_ISDNCallVolume	Summarizes the average ISDN channel call volume for the links on selected devices.
Report_ISDNTimeDetail	Summarizes the average ISDN statistics on selected trunks.
Report_ISDNUtilization	Summarizes the average ISDN channel call volume for the trunks on selected devices.
Report_LinkUtilization	Summarizes average link usage.
Report_QoSUtilization	Summarizes average traffic class statistics for the links on selected devices.
Report_QoSVolume	Summarizes average traffic class statistics for the links on selected devices.
Report_TotalVolume	Summarizes total volume for selected devices.
SingleATMLink_Util	Monitors the usage of the ATM links on a single network device.
SingleFrameRelayLink_Util	Monitors the usage of frame relay links on a single network device.
SingleInterface_Health	Monitors the health of interfaces on a single network device.
SingleLANLink_Util	Monitors the usage of the LAN links on a single network device.
SingleWANLink_Util	Monitors the usage of the serial, T1, or T3 links on a single network device.
SNMPTrap_AddMIB	Add management information bases for monitoring by the SNMPTrap_Async Knowledge Script.
SNMPTrap_Async	Checks for incoming SNMP traps forwarded from NetIQ SNMP Trap Receiver.
WANLink_QoS	Monitors QoS on WAN links on a Cisco IOS device for traffic class usage, dropped packet rate, and queue depth.

Knowledge Script	What It Does
WANLink_Util	Monitors the parent resource for the serial, T1, or T3 links on a network device.
Recommended Knowledge Scripts	Identifies the scripts recommended for optimal monitoring of network devices.

3.1 ATMLink_QoS

Use this Knowledge Script to monitor Quality of Service (QoS) on ATM links on a Cisco IOS device. This script monitors traffic class usage, dropped packet rate, and queue depth. In addition, this script raises an event if a monitored item exceeds the threshold that you set and generates datastreams for all monitored items.

Traffic class

A particular category of traffic on an interface. For example, voice and data can be classified as individual traffic classes.

Queue

The virtual buffer associated with a particular traffic class.

Dropped packet rate

The rate at which packets are dropped because of factors such as queuing, policing, early detection, or traffic shaping.

Queue depth

The number of packets in a queue.

Policy

The action that QoS takes within a traffic class upon the traffic that enters the class, such as dropping packets. Pre-policy traffic is the traffic that flows into a traffic class, before QoS applies a policy. Post-policy is the traffic that leaves a traffic class after a policy has been applied.

Resource Object

NetworkDevice ATM Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	

Parameter	How to Set It
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the ATMLink_QoS job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Link name filter	Using regular expression, specify the names of the ATM links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** ◆ To monitor all ATM links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude interface name filter.* ◆ To monitor all ATM links, enter `"*"` and select **Include** in *Include or exclude link name filter*. ◆ To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the ATM links you specified in *Link name filter*. Select **Exclude** to monitor all ATM links except those you specified in *Link name filter.*
Class name filter	Using regular expression, specify the names of the traffic classes you want to monitor. Leave this parameter blank to monitor all traffic classes.
Traffic Class Utilization	
Monitor traffic class utilization?	Select **Yes** to monitor traffic class usage and to activate the parameters in this section. The default is Yes.
Collect data for traffic class utilization?	Select **Yes** to collect data for charts and graphs. The default is No. This script generates datastreams for the pre-policy and post-policy bandwidth used by each configured traffic class.
Threshold - Maximum traffic class utilization	Specify the highest percentage of traffic class usage that can occur before an event is raised. The default is 25%.
Event severity when traffic class utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of traffic class usage exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.

Parameter	How to Set It
Collect data for traffic class pre/post policy bytes?	Select **Yes** to collect data for charts and graphs. The default is No. This script creates datastreams for the number of pre- and post-policy bytes per second.
Select unit for traffic class pre/post policy bytes	Select the unit for collecting data for the pre/post policy bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Queue Depth	
Monitor queue depth?	Select **Yes** to monitor queue depth and to activate the parameters in this section. The default is Yes.
Collect data for queue depth?	Select **Yes** to collect data for charts and graphs. The default is No. This script generates datastreams for queue depth (number of packets) by class name.
Threshold - Maximum priority queue depth	Specify the maximum number of packets that a priority queue can contain before an event is raised. The default is 0 packets.
Threshold - Maximum non-priority queue depth	Specify the highest number of packets that a non-priority queue can contain before an event is raised. The default is 10 packets.
Event severity when queue depth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the queue depth exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Dropped Packets	
Monitor dropped packet rate?	Select **Yes** to monitor the rate at which packets are dropped from the traffic class and to activate the parameters in this section. The default is Yes.
Collect data for dropped packet rate?	Select **Yes** to collect data for charts and graphs. the default is No. This script generates datastreams for the percentage of dropped packets, and for the number of packets dropped per second.
Threshold - Maximum dropped packet rate	Specify the maximum rate at which packets can be dropped from the traffic class before an event is raised. The default is 1%.
Event severity when dropped packet rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the dropped packet rate exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.2 ATMLink_Util

Use this Knowledge Script to monitor the usage of the parent resource of the Asynchronous Transfer Mode (ATM) links on a network device. This script raises an event if a monitored value exceeds the threshold that you set. In addition, this script generates datastreams for bandwidth usage, packet rate, and packet error rate.

NOTE: ATMLink_Util differs from SingleATMLink_Util in that it lets you monitor all links for all devices of any parent resource. SingleATMLink_Util allows you to monitor selected links for only one device.

You should understand your network's normal behavior so that you know when to examine usage levels more closely.

Determine usage levels on your current network: ethernet, Fiber Distributed Data Interface (FDDI), token ring, and Asynchronous Transfer Mode (ATM). On most networks, usage gradually increases as users begin using more network resources, such as email, network printing, and file sharing. Be concerned with usage peaks that *do not* follow this pattern.

Examine your network's typical usage over time and note whether your network has experienced a gradual or sudden increase in usage.

- A sharp increase in usage indicates an abnormal condition. Search the area of the network where the increase occurred. For example, a device may be causing "broadcast storms."
- A sustained high or low level of usage indicates an increasing or decreasing load on your network. If necessary, redistribute network traffic by segmenting your LAN with a bridge, router, or switch.

Resource Object

NetworkDevice ATM Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the ATMLink_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.

Parameter	How to Set It
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Link name filter	Using regular expression, specify the names of the ATM links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** ◆ To monitor all ATM links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* ◆ To monitor all ATM links, enter "*" and select **Include** in *Include or exclude link name filter.* ◆ To monitor nothing, enter "*" and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the ATM links you specified in *Link name filter*. Select **Exclude** to monitor all ATM links except those you specified in *Link name filter.*
Link Utilization	
Monitor link utilization?	Select **Yes** to monitor link usage and to activate the parameters in this section. The default is Yes.
Collect data for bandwidth utilization?	Select **Yes** to collect data about bandwidth usage for charts and graphs. The default is Yes.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Select **Yes** to collect data about sent and received bytes for charts and graphs. The default is Yes.
Select unit for bytes sent/received	Select the unit for collecting data for the sent/received bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Collect data for inbound/outbound bandwidth utilization?	Select **Yes** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is No.
Link Errors	
Monitor link errors?	Select **Yes** to monitor link errors and to activate the parameters in this section. The default is Yes.

Parameter	How to Set It
Collect data for link errors?	Select **Yes** to collect data about link errors for charts and graphs. The default is No.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 50%.
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.3 Chassis_Usage

Use this Knowledge Script to monitor the physical chassis of a network device and create datastreams for the following:

- CPU usage
- Memory buffer error rate
- Backplane usage
- Voltage values
- Fan status
- Memory poll usage
- Flash memory usage
- Temperature values
- Power supply status

This script raises an event if any value exceeds a specified threshold. In addition, this script generates datastreams for CPU usage, RAM usage, flash memory usage, backplane usage, temperature and voltage states, and power supply and fan status.

Troubleshooting Events

The topic discusses possible causes and corrective actions for events that are raised when usage exceeds the threshold you set. You should understand your network's normal behavior so that you know when to examine usage levels more closely.

Determine usage levels on your current network: ethernet, Fiber Distributed Data Interface (FDDI), token ring, and Asynchronous Transfer Mode (ATM). On most networks, usage gradually increases as users begin using more network resources, such as email, network printing, and file sharing. Be concerned with usage peaks that *do not* follow this pattern.

Examine your network's typical usage over time and note whether your network has experienced a gradual or sudden increase in usage.

- A sharp increase in usage indicates an abnormal condition. Search the area of the network where the increase occurred. For example, a device may be causing "broadcast storms."
- A sustained high or low level of usage indicates an increasing or decreasing load on your network. If necessary, redistribute network traffic by segmenting your LAN with a bridge, router, or switch.

Resource Object

NetworkDevice Chassis Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Chassis_Usage job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
CPU	
Monitor CPU?	Select **Yes** to monitor CPU usage and to activate the parameters in this section. The default is Yes.
Collect data for CPU utilization?	Select **Yes** to collect data about CPU usage for charts and reports. The default is Yes.mum percentage of CPU usage that can occur before an event i
Threshold - Maximum CPU utilization	Specify the maxis raised. The default is 50%.

Parameter	How to Set It
Event severity when CPU utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which CPU usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive CPU usage. The default is 10.
RAM	
Monitor RAM?	Select **Yes** to monitor RAM usage and to activate the parameters in this section. The default is Yes. RAM usage includes NVRAM, DRAM, and SRAM, depending on whether you are monitoring a switch or a router.
Collect data for RAM utilization?	Select **Yes** to collect data about RAM usage for charts and reports. The default is Yes.
Threshold - Maximum memory pool utilization	Specify the maximum percentage of memory pool usage that can occur before an event is raised. The default is 50%.This figure represents the maximum usage for all memory pools (NVRAM, DRAM, and SRAM).
Event severity when memory pool utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which memory pool usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive memory pool usage. The default is 10.
Threshold - Maximum memory buffer error rate	Specify the maximum number of memory buffer errors that can occur per second before an event is raised. The default is 0.
Event severity when memory buffer error rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the number of memory buffer errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive memory buffer error rate. The default is 10.
Flash Memory	
Monitor flash memory?	Select **Yes** to monitor flash memory and to activate the parameters in this section. The default is Yes.
Collect data for flash memory utilization?	Select **Yes** to collect data about flash memory usage for charts and reports. The default is No.
Threshold - Maximum flash memory utilization	Specify the maximum percentage of flash memory usage that can occur before an event is raised. The default is 90%.
Event severity when flash memory utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which flash memory usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive flash memory usage. The default is 10.
Backplane	
Monitor backplane?	Select **Yes** to monitor backplane usage and to activate the parameters in this section. The default is Yes.
Collect data for backplane utilization?	Select **Yes** to collect data about backplane usage for charts and reports. The default is Yes.
Threshold - Maximum backplane utilization	Specify the maximum percentage of backplane usage that can occur before an event is raised. The default is 75%.

Parameter	How to Set It
Event severity when backplane utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which backplane usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive backplane usage. The default is 10.
Temperature Sensors	
Monitor temperature sensors?	Select **Yes** to monitor temperature sensors and to activate the parameters in this section. The default is Yes.
Collect data for temperature?	Select **Yes** to collect data about temperature states for charts and reports. The default is No.
Threshold - Maximum temperature	Specify the maximum temperature that can be reached before an event is raised. The default is 50 degrees Celsius.
Event severity when temperature exceeds threshold or sensor state not OK	Set the severity level, between 1 and 40, to indicate the importance of an event in which the temperature exceeds the threshold that you set or if the state of the temperature sensor is not "OK." Enter **0** if you do not want to raise an event. The default is 10.
Voltage Sensors	
Monitor voltage sensors?	Select **Yes** to monitor voltage sensors and to activate the parameters in this section. The default is Yes.
Collect data for voltage sensor state?	Select **Yes** to collect data about voltage states for charts and reports. The default is No.
Event severity when voltage state not OK	Set the severity level, between 1 and 40, to indicate the importance of an event in which the voltage state is not "OK." The default is 10.
Power Supplies	
Monitor power supplies?	Select **Yes** to monitor power supplies and to activate the parameters in this section. The default is Yes.
Collect data for power supply state?	Select **Yes** to collect data about power supply states for charts and reports. The default is No.
Event severity when power supply state not OK	Set the severity level, between 1 and 40, to indicate the importance of an event in which the power supply state is not "OK." The default is 10.
Fans	
Monitor fans?	Select **Yes** to monitor fans and to activate the parameters in this section. The default is Yes.
Collect data for fan state?	Select **Yes** to collect data about fan states for charts and reports. The default is No.
Event severity when fan state not OK	Set the severity level, between 1 and 40, to indicate the importance of an event in which the fan state is not "OK." The default is 10.
DSP Cards	
Monitor DSP cards?	Select **Yes** to monitor DSP (Digital Signal Processing) cards and to activate the parameters in this section. The default is Yes. DSP cards provide transcoding functionality between the PSTN and IP network.
Collect data for DSP card utilization?	Select **Yes** to collect data about DSP card resource usage and status. The default is No.

Parameter	How to Set It
Maximum DSP card utilization	Specify the maximum percentage of DSP card usage that can occur before an event is raised. The default is 75%.
Event severity when DSP card utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which DSP card usage exceeds the threshold that you set. The default is 10.
Event severity when DSP card state not OK	Set the severity level, between 1 and 40, to indicate the importance of an event in which the DSP card state is not "Normal." Events will be raised for the following states: **Warning**, **Critical**, **Fatal**, and **offLine**. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to No.

3.4 Device_Ping

Use this AppManager for Network DevicesKnowledge Script to check the availability of network devices that respond to Internet Control Message Protocol (ICMP) Echo requests. This script raises an event if any value exceeds a specified threshold. In addition, this script generates datastreams for device Coexisting with Microsoft SNMP Trap Serviceavailability.

Resource Object

NetworkDevice

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General	
Collect data for device availability?	Select **Yes** to collect data about timeouts and echo requests for charts and graphs. The default is Yes.
Event severity when ping test fails	Set the severity level, between 1 and 40, to indicate the importance of an event in which a ping test fails. For example, a ping test could fail because the command is not found or because a device's IP address is incorrect. The default is 5.

Parameter	How to Set It
Echo Settings	
Number of echo requests to send	Specify the number of times to send the ping echo request per job iteration. The default is 3 requests.
Number of seconds before timeout	Specify the maximum number of seconds to wait for a response before timing out ping echo request. The default is 3 seconds.
Maximum number of request timeouts	Specify the maximum number of ping echo request timeouts that you want to allow before raising an event. The default is 1 timeout
Require request timeouts to be consecutive?	Select **Yes** if you want the number of ping echo request timeouts to be consecutive before raising an event. For example, you select Yes for this parameter, specify the *Maximum number of request timeouts* to be 2, and specify the *Number of echo requests to send* to be 3. When you run this script, if the first echo request succeeds and second and third echo requests fail, then AppManager raises an event. On the other hand, if the first echo request fails, the second echo request succeeds, and the third echo request fails, then AppManager does not raise an event. If you want to raise an event after the specified number of request timeouts, and the failure need not be consecutive, then select No. The default is Yes.
Consecutive job iterations before raising event	Specify the number of job iterations the script should run consecutively before raising an event. The default is 1 job iteration. For example, specify 2 for this parameter and run this script. Assume that in the first and second iteration, the job meets the specified event condition. In this case, AppManager raises an event in the second iteration. Then in the third iteration, if the job meets the event condition, AppManager raises an event again. On the fourth iteration, if the job does not meet the specified event condition, then AppManager does not raise an event. AppManager raises further events only on the iteration when the event condition is met consecutively following the iterations where the event condition is not met. For example, on the fifth and sixth iteration, if the job meets the specified event criteria, AppManager raises an event in the sixth iteration.

3.5 Device_Syslog

Syslog is a notification system by which devices on a network, such as routers, switches, and even hosts, can send notifications and alerts to a central server. Syslog traffic is transported by UDP over port 514. Use this Knowledge Script to listen for UDP traffic on port 514.

When you change a parameter value in the script while the job is running, the job stops and immediately restarts. It is possible for the job to restart before Windows has a chance to free the port 514. Therefore, the script job will fail on restart because it cannot listen on the Syslog port. You should wait 5 seconds or so before restarting the job. Waiting gives Windows a chance to free the port for listening.

Because AppManager performs active SNMP polling as well as passive Syslog monitoring, you may receive event notifications from both sources. For example, SNMP polling alerts AppManager when an interface goes down and, as a result, you receive an AppManager event. In addition, you may receive a Syslog message that provides the same information.

Prerequisite

Before using the Device_Syslog Knowledge Script, configure your network devices to send Syslog messages to the proxy agent computer. Configuration procedures are device specific. Consult the documentation for your particular device. The following procedure is for Cisco devices.

To configure Cisco devices:

1. Telnet to the device you want to configure.
2. Type the requested password and press [`Enter`].
3. Type `enable` and press [`Enter`].
4. Type the requested password and press [`Enter`].
5. Type `config` and press [`Enter`].
6. Type `logging` *<host name or IP address of device that you want to configure>*.
7. Exit.

Resource Object

NetworkDevice

Because this script listens on port 514, run this script only once on a proxy agent computer.

Default Schedule

By default, this script runs on an asynchronous schedule in order to report events as they occur. Once you start the Knowledge Script, its job status is “Running” and will remain so until you stop the job.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General	
Has the most commonly used panels minimized on the right side	Has the most commonly used panels minimized on the right side
Has the most commonly used panels minimized on the right side	Has the most commonly used panels minimized on the right side
Has the most commonly used panels minimized on the right side	Has the most commonly used panels minimized on the right side

Parameter	How to Set It
Monitor Syslog messages from all devices?	Select **Yes** to accept all Syslog messages from all devices, including messages from devices that are not in the TreeView pane. If a device is in the TreeView pane, events are raised against the device. If a device is not in the TreeView pane, events are raised against the proxy agent computer. Select **No** to monitor Syslog messages only from those devices on which you run this script. The default is No.
Message text filter	Using regular expression, provide the text you want to find in the Syslog. Leave this parameter blank to find all text.
Event severity when error messages found	Set the severity level, between 1 and 40, to indicate the importance of an event in which error messages are found in the log. The default is 5. Set the severity level to **0** if you do not want to raise an event.
Event severity when warning messages found	Set the severity level, between 1 and 40, to indicate the importance of an event in which warning messages are found in the log. The default is 15. Set the severity level to **0** if you do not want to raise an event.
Event severity when informational messages found	Set the severity level, between 1 and 40, to indicate the importance of an event in which informational messages are found in the log. The default is 0. Set the severity level to **0** if you do not want to raise an event.

3.6 Device_Uptime

Use this Knowledge Script to monitor one of the following:

- The number of hours that a network device has been operational since it was last restarted.
- The number of hours that a device's network management component, such as the SNMP agent, has been operational since it was last restarted.

This script raises an event if the device is restarted during the monitoring interval. In addition, this script generates datastreams for device uptime.

In the event of a device restart, you can set an action on the Actions tab to automatically run the Action_RunDiscoveryNetworkDevice Knowledge Script. The Action script discovers network device resources on the rebooted device.

Resource Object

NetworkDevice

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Device_Uptime job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Collect data for uptime?	Select **Yes** to collect data about uptime for charts and graphs. The default is No. This script generates a datastream for the number of hours that a device has been operational since its last reboot or for the number of hours that the management component has been operational since its last restart. The datastream legend is the same for host or management component: "`Device uptime [<device>] (hours)`"
Monitor host uptime or uptime of the network management portion of the system	Select whether to monitor the device itself or the device's management component: ◆ Select **Host uptime** to monitor the uptime of a host device. ◆ Select **Management component uptime** to monitor the management component of a device, independent of the uptime of the host device.
Event severity when device reboots	Set the severity level, between 1 and 40, to indicate the importance of an event in which the monitored device has been rebooted. Set the severity level to **0** if you do not want to raise an event. The default severity level is 5.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.7 FrameRelayLink_QoS

Use this Knowledge Script to monitor Quality of Service (QoS) on frame relay links on a Cisco IOS device. This script monitors traffic class usage, dropped packet rate, and queue depth. This script raises an event if a monitored item exceeds the threshold that you set and generates datastreams for traffic class usage, dropped packet rates, and queue depth by class name.

Traffic class

A particular category of traffic on an interface. For example, voice and data can be classified as individual traffic classes.

Queue

The virtual buffer associated with a particular traffic class.

Dropped packet rate

The rate at which packets are dropped because of factors such as queuing, policing, early detection, or traffic shaping.

Queue depth

The number of packets in a queue.

Policy

The action that QoS takes within a traffic class upon the traffic that enters the class, such as dropping packets. Pre-policy traffic is the traffic that flows into a traffic class, before QoS applies a policy. Post-policy refers to the traffic that leaves a traffic class after a policy has been applied.

Resource Object

NetworkDevice FR Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the FrameRelayLink_QoS job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	

Parameter	How to Set It
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Link name filter	Using regular expression, specify the names of the frame relay links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** ◆ To monitor all frame relay links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* ◆ To monitor all frame relay links, enter `"*"` and select **Include** in *Include or exclude link name filter.* ◆ To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter.* ◆ To monitor only serial links, enter `(?=serial)` and select **Include** in *Include or exclude link name filter.* ◆ To monitor all interfaces EXCEPT serial links, enter `(?=serial)` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the frame relay links you specified in *Link name filter*. Select **Exclude** to monitor all frame relay links except those you specified in *Link name filter.*
Class name filter	Using regular expression, specify the name of the traffic classes that you want to monitor. Leave this parameter blank to monitor all traffic classes.
Traffic Class Utilization	
Monitor traffic class utilization?	Select **Yes** to monitor traffic class usage and to activate the parameters in this section. The default is Yes.
Collect data for traffic class utilization?	Select **Yes** to collect data for charts and graphs. The default is No. This script creates datastreams for the pre-policy and post-policy bandwidth used by each configured traffic class.
Threshold - Maximum traffic class utilization	Specify the maximum percentage of traffic class usage that can occur before an event is raised. The default is 25%.
Event severity when traffic class utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of traffic class usage exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Collect data for traffic class pre/post policy bytes?	Select **Yes** to collect data for charts and graphs. The default is No. This script creates datastreams for the number of pre-policy and post-policy bytes per second.

Parameter	How to Set It
Select unit for traffic class pre/post policy bytes	Select the unit for collecting data for the pre/post policy bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Queue Depth	
Monitor queue depth?	Select **Yes** to monitor queue depth and to activate the parameters in this section. The default is Yes.
Collect data for queue depth?	Select **Yes** to collect data for charts and graphs. The default is No. This script generates datastreams for queue depth (number of packets) by class name.
Threshold - Maximum priority queue depth	Specify the maximum number of packets that a priority queue can contain before an event is raised. The default is 0 packets.
Threshold - Maximum non-priority queue depth	Specify the highest number of packets that a non-priority queue can contain before an event is raised. The default is 10 packets.
Event severity when queue depth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the queue depth exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Dropped Packets	
Monitor dropped packet rate?	Select **Yes** to monitor the rate at which packets are dropped from the traffic class and to activate the parameters in this section. The default is Yes.
Collect data for dropped packet rate?	Select **Yes** to collect data for charts and graphs. The default is No.This script generates datastreams for the percentage of dropped packets, and for the number of packets dropped per second.
Threshold - Maximum dropped packet rate	Specify the maximum rate at which packets can be dropped from the traffic class before an event is raised. The default is 1%.
Event severity when dropped packet rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the dropped packet rate exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.8 FrameRelayLink_Util

Use this Knowledge Script to monitor the usage of a parent resource for the frame relay links on a network device. A frame relay link uses a packet-switching protocol for connecting devices on a Wide Area Network (WAN). This script raises an event if a monitored value exceeds the threshold you set. In addition, this script generates datastreams for the following:

- Bandwidth usage
- Frame rate

- FECN (Forward Explicit Congestion Notification) rate. A *FECN* is a frame relay message that notifies the receiving device when there is congestion in the network. A FECN bit is sent in the direction in which the frame is traveling, toward its destination.
- BECN (Backward Explicit Congestion Notification) rate. A *BECN* is a frame relay message that notifies the sending device when there is congestion in the network. A BECN bit is sent in the direction from which the frame is traveling, toward its transmission source.

NOTE: FrameRelayLink_Util differs from SingleFrameRelayLink_Util in that it lets you monitor all links for all devices of any parent resource. SingleFrameRelayLink_Util allows you to monitor selected links for only one device.

Resource Object

NetworkDevice FR Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the FrameRelayLink_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.

Parameter	How to Set It
Link name filter	Using regular expression, specify the names of the frame relay links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** ◆ To monitor all frame relay links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* ◆ To monitor all frame relay links, enter `"*"` and select **Include** in *Include or exclude link name filter.* ◆ To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter.* ◆ To monitor only serial links, enter `(?=serial)` and select **Include** in *Include or exclude link name filter.* ◆ To monitor all interfaces EXCEPT serial links, enter `(?=serial)` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the frame relay links you specified in *Link name filter*. Select **Exclude** to monitor all frame relay links except those you specified in *Link name filter.*
Link Utilization	
Monitor link utilization?	Select **Yes** to monitor link usage and to activate the parameters in this section. The default is Yes.
Collect data for link bandwidth utilization?	Select **Yes** to collect data about bandwidth usage for charts and graphs. The default is Yes.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Select **Yes** to collect data about sent and received bytes for charts and graphs. The default is Yes.
Select unit for bytes sent/received	Select the unit for collecting data for the sent/received bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Collect data for inbound/outbound bandwidth utilization?	Select **Yes** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is No.
Link Errors	
Monitor FECNs/BECNs?	Select **Yes** to monitor FECN and BECN rates and to activate the parameters in this section. The default is Yes.
Collect data for FECNs/BECNs?	Select **Yes** to collect data about FECN and BECN rates for charts and graphs. The default is No.

Parameter	How to Set It
Threshold - Maximum FECNs/BECNs	Specify the maximum percentage of FECN/BECN rates that can occur before an event is raised. The default is 8%.
Event severity when FECNs/BECNs exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of FECN/BECN rates exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.9 FXOPort_Health

Use this Knowledge Script to monitor signal errors on a Foreign Exchange Office (FXO) port on a network device. This script raises an event if the number of signal errors exceeds the specified threshold. In addition, this script generates datastreams for signal errors.

Resource Object

NetworkDevice FXO Port Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the FXOPort_Health job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.

Parameter	How to Set It
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Collect data for signal errors?	Select **Yes** to collect data about signal errors for charts and graphs. The default is No.
Threshold - Maximum signal errors	Specify the maximum number of signal errors that can occur before an event is raised. The default is 0 errors.
Event severity when signal errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the number of signal errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive signal errors. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.10 FXOPort_Util

Use this Knowledge Script to monitor Foreign Exchange Office (FXO) port usage on a network device. This script raises an event if port usage exceeds the specified threshold. In addition, this script generates datastreams for port usage.

Resource Object

NetworkDevice FXO Port Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the FXOPort_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.

Parameter	How to Set It
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Collect data for FXO port utilization?	Select **Yes** to collect data about port usage for charts and graphs. The default is Yes.
Threshold - Maximum FXO port utilization	Specify the maximum percentage of port usage that can occur before an event is raised. The default is 80%.
Event severity when port utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which port usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for port usage. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.11 FXSPort_Health

Use this Knowledge Script to monitor signal errors on a Foreign Exchange Station (FXS) port on a network device. This script raises an event if the number of signal errors exceeds the specified threshold. In addition, this script generates datastreams for signal errors.

Resource Object

NetworkDevice FXS Port Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	

Parameter	How to Set It
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the FXSPort_Health job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Collect data for signal errors?	Select **Yes** to collect data about signal errors for charts and graphs. The default is No.
Threshold - Maximum signal errors	Specify the maximum number of signal errors that can occur before an event is raised. The default is 0 errors.
Event severity when signal errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the number of signal errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive signal errors. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.12 FXSPort_Util

Use this Knowledge Script to monitor Foreign Exchange Station (FXS) port usage on a network device. This script raises an event if port usage exceeds the specified threshold. In addition, this script generates datastreams for port usage.

Resource Object

NetworkDevice FXS Port Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the FXSPort_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Collect data for FXS port utilization?	Select **Yes** to collect data about port usage for charts and graphs. The default is Yes.
Threshold - Maximum FXS port utilization	Specify the maximum percentage of port usage that can occur before an event is raised. The default is 80%.
Event severity when port utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which port usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for port usage. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.13 Host_CPULoaded

Use this Knowledge Script to access the Host Resource MIB to monitor CPU usage on a host device. This script raises an event if CPU usage exceeds the threshold that you set. In addition, this script generates a datastream for percentage of CPU usage during the monitoring period.

NOTE: For a Nortel CS1000 version 4.5 Call Server, this script monitors call capacity usage rather than CPU usage. In version 4.5 devices, the MIB value for the CPU processor load represents call capacity usage.

Resource Object

NetworkDevice Host Processor

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Host_CPULoaded job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Collect data for CPU utilization?	Select **Yes** to collect data for charts, graphs, and reports. When enabled, data collection returns the overall CPU usage percentage. The default is No.
Threshold - Maximum CPU utilization	Specify the maximum CPU usage that must occur before an event is raised. The default is 50%.
Event severity when CPU utilization exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. If you do not want to raise an event, set the severity level to **0**. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. If you set this parameter to Yes, then AppManager raises an event when a particular performance counter cannot be found in an iteration. For example, if this script does not find a particular performance counter in the first iteration, AppManager raises an event on the first iteration and does not raise further events for consecutive failures. This script raises further one-time events only on the iteration when there are failure events following successful retrieval of the performance counters. If you do not want to see such one-time events, set this parameter to **No**.

3.14 Host_DeviceStatus

Use this Knowledge Script to access the Host Resource MIB to monitor the status of a device and the number of errors that have occurred since the last iteration of the script. This script raises an event if a device is down or if errors occur. In addition, this script generates datastreams for device status and the number of errors.

NOTE: This script retrieves the error count from the DeviceErrors field of the Host Resource MIB.

Resource Object

NetworkDevice Host Device

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Host_DeviceStatus job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Raise event if device is down?	Select **Yes** to raise an event if the monitored device is down. The default is Yes.
Event severity when device is down	Set the severity level, between 1 and 40, to indicate the importance of an event in which the monitored device is down. The default is 10.
Collect data for device status?	Select **Yes** to collect data for charts, graphs, and reports. When enabled, data collection returns 100 if the device is up or 0 if the device is down. The default is No.

Parameter	How to Set It
Raise event if device errors occur?	Select **Yes** to raise an event if errors occurred since the last iteration of the script. The default is Yes.
Event severity when device errors occur	Set the severity level, between 1 and 40, to indicate the importance of an event in which errors occurred since the last iteration of the script. The default is 10.
Collect data for device errors?	Select **Yes** to collect data for charts, graphs, and reports. When enabled, data collection returns a datastream for the number of errors that have occurred since the last iteration of the script. The default is No.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. If you set this parameter to Yes, then AppManager raises an event when a particular performance counter cannot be found in an iteration. For example, if this script does not find a particular performance counter in the first iteration, AppManager raises an event on the first iteration and does not raise further events for consecutive failures. This script raises further one-time events only on the iteration when there are failure events following successful retrieval of the performance counters. If you do not want to see such one-time events, set this parameter to No.

3.15 Host_MemoryUsage

Use this Knowledge Script to access the Host Resource MIB to monitor memory usage on a device. This script raises an event if memory usage exceeds the threshold you set. In addition, this script generates a datastream for memory usage on the device.

Resource Object

NetworkDevice Host Memory

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Host_MemoryUsage job. The default is 5.

Parameter	How to Set It
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Collect data for memory usage?	Select **Yes** to collect data for charts, graphs, and reports. When enabled, data collection returns the percentage of memory usage for the monitoring period. The default is No.
Threshold - Maximum memory usage	Specify the maximum memory usage that must occur before an event is raised. The default is 90%.
Event severity when memory usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. If you do not want to raise an event, set the severity level to **0**. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. If you set this parameter to Yes, then AppManager raises an event when a particular performance counter cannot be found in an iteration. For example, if this script does not find a particular performance counter in the first iteration, AppManager raises an event on the first iteration and does not raise further events for consecutive failures. This script raises further one-time events only on the iteration when there are failure events following successful retrieval of the performance counters. If you do not want to see such one-time events, set this parameter to No.

3.16 Host_ProcessDown

Use this Knowledge Script to access the Host Resource MIB to determine whether specified processes are not running. This script raises an event if a specified process is not running. In addition, this script generates datastreams for process status.

Resource Object

NetworkDevice Host Processor Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Host_ProcessDown job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Enable use of SNMP GETBulk operations?	Select **Yes** to enable SNMP GETBulk operations. GETBulk operation requests a number of GETNEXT responses to be returned in a single packet than issuing multiple GETNEXT operations. The GETBulk operation uses less bandwidth and optimizes the agent in retrieving the data from MIB instrumentation. The default is unselected.
Number of row to request for each GETBulk operation	Specify the number of rows that should be retrieved for each GETBulk operation. You can specify a maximum of 200 rows. The default is 10.
Raise event if process is not running?	Select **Yes** to raise an event if a specified process is not running. The default is Yes.
Processes to monitor	Specify one or more process names, separated by commas and no spaces. For example: `grep.exe,batch.exe` **NOTE:** If the device being monitored is running on Microsoft Windows, the process name specified should match the Image Name seen on the Process tab in Task Manager.
Collect data for process status?	Select **Yes** to collect data for charts and reports on status of process. If you enable this parameter, data collection returns a value of 100 when a specified process is running, or a value of 0 when the process is not running. Selecting this parameter collects data for all the processes that are being monitored. The default is unselected.
Limit process status data collection to specific list	Select Yes to collect data for chart and reports for specific processes. Selecting this parameter collect data only for specific processes specified in the *Process to collect data for* parameter.

Parameter	How to Set It
Process to collect data for (comma-separated)	Specify one or more process names, separated by commas and no spaces for which you want to collect data. You must specify at least one process if you selected the *Limit process status data collection to specific list* parameter. For example, if you are monitoring proc1, proc2, and proc3 but has not specified any process for this parameter, then the data will be collected for all the processes that are being monitored. Also, events will be generated if any of these processes are down. On the other hand, if you are monitoring proc1, proc2, and proc3 and specify the data collection for proc3, proc4, and proc5, then event will be generated for proc1, proc2 and proc3 if any of these processes are down. But, data will be collected only for proc3, proc4, and proc5. **NOTE:** The process name that you specify should match the process name running on a device.
Event severity when process is not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which specified processes are not running. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. If you set this parameter to Yes, then AppManager raises an event when a particular performance counter cannot be found in an iteration. For example, if this script does not find a particular performance counter in the first iteration, AppManager raises an event on the first iteration and does not raise further events for consecutive failures. This script raises further one-time events on the iteration when there are failure events following successful retrieval of the performance counters. If you do not want to see such one-time events, set this parameter to **No**.

3.17 Host_ProcessUp

Use this Knowledge Script to access the Host Resource MIB to verify whether a specified process is running. This script raises an event if a specified process is running and generates datastreams for process status.

Resource Object

NetworkDevice Host Processor Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Host_ProcessUp job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Enable use of SNMP GETBulk operations?	Select **Yes** to enable SNMP GETBulk operations. GETBulk operation requests a number of GETNEXT responses to be returned in a single packet than issuing multiple GETNEXT operations. The GETBulk operation uses less bandwidth and optimizes the agent in retrieving the data from MIB instrumentation. The default is unselected.
Number of row to request for each GETBulk operation	Specify the number of rows that should be retrieved for each GETBulk operation. You can specify a maximum of 200 rows. The default is 10.
Raise event if process is running?	Select **Yes** to raise an event if a specified process is running. The default is Yes.
Collect data for process status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns a value of 100 when a specified process is running, or a value of 0 when the process is not running. The default is No.
Processes to monitor	Specify one or more process names, separated by commas and no spaces. For example: `grep.exe,batch.exe` **NOTE:** If the device being monitored is running on Microsoft Windows, the process name specified should match the Image Name seen on the **Process** tab in Task Manager.
Event severity when process is running	Set the severity level, from 1 to 40, to indicate the importance of an event in which the specified processes are running. The default is 10.

Parameter	How to Set It
Raise one-time events?	Select **Yes** to raise an event for all one-time events. If you set this parameter to Yes, then AppManager raises an event when a particular performance counter cannot be found in an iteration. For example, if this script does not find a particular performance counter in the first iteration, AppManager raises an event on the first iteration and does not raise further events for consecutive failures. This script raises further one-time events only on the iteration when there are failure events following successful retrieval of the performance counters. If you do not want to see such one-time events, set this parameter to **No**.

3.18 Host_StorageUsage

Use this Knowledge Script to access the Host Resource MIB to monitor storage usage on a device. This script raises an event if storage usage exceeds the threshold that you set. In addition, this script generates a datastream for storage usage on the device.

Resource Object

NetworkDevice Host Storage

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Host_StorageUsage job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.

Parameter	How to Set It
Collect data for storage usage?	Select **Yes** to collect data for charts, graphs, and reports. When enabled, data collection returns the percentage of storage usage for the monitoring period. The default is No.
Threshold - Maximum storage usage	Specify the maximum storage usage that can occur before an event is raised. The default is 90%.
Event severity when storage usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which storage usage exceeds the threshold. If you do not want to raise an event, set the severity level to **0**. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. If you set this parameter to Yes, then AppManager raises an event when a particular performance counter cannot be found in an iteration. For example, if this script does not find a particular performance counter in the first iteration, AppManager raises an event on the first iteration and does not raise further events for consecutive failures. This script raises further one-time events only on the iteration when there are failure events following successful retrieval of the performance counters. If you do not want to see such one-time events, set this parameter to No.

3.19 Interface_Health

Use this Knowledge Script to monitor the parent resource for the interfaces on a network device. This script raises an event if the interface status changes or if any value exceeds a specified threshold. This script generates datastreams indicating the number of “up” interfaces and the total number of interfaces.

NOTE: Interface_Health differs from SingleInterface_Health in that it lets you monitor all interfaces for all devices of any parent resource. SingleInterface_Health allows you to monitor selected interfaces for only one device.

Troubleshooting Events

The table below identifies possible causes and corrective actions for events that are raised when an interface’s status changes. These events can lead to unacceptable service levels for an interface that remains down.

Narrow the usage problem to ports that have excessively high or low usage. If necessary, redistribute network traffic by segmenting your LAN with a bridge, router, or switch.

Determine usage levels on your current network. Try to locate the segments that are experiencing high or low usage levels, which are an indicator of the usage on the chassis.

Possible Cause	Corrective Action
No cable connected	Reconnect the cable on the switch to a known good device.
Wrong port	Ensure both ends of the cable are plugged into the correct ports.

Possible Cause	Corrective Action
Device has no power	Ensure both devices are powered on and connected to a power source.
Wrong cable type	Verify your cable selection.
Bad cable	Swap the suspect cable with a known good cable. Look for broken or missing pins on the connector.
Loose connections	Unplug a cable and reinsert it. A cable may not be as fully seated in a jack as it appears.
Patch panels	Eliminate faulty patch panel connections. If possible, bypass the patch panel to rule it out as a possible cause.
Media convertors	Eliminate faulty media convertors, such as fiber-to-copper. If possible, bypass the media convertor to rule it out as a possible cause.
Bad or wrong gigabit	Swap the suspect GBOC with a known good GBIC.
Interface convertor (GBIC)	Verify hardware and software support for this type of GBIC.
Bad port or module	Move the cable to a known good port to troubleshoot a suspect port or module.
Port, interface, or module not enabled	Use the `show port` command for CatOS or the `show interface` command for Cisco IOS to look for errdisable, disable, or shutdown status. Use the `show module` command to look for faulty status, which could indicate a hardware problem.

Resource Object

NetworkDevice Interface Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Interface_Health job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	

Parameter	How to Set It
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Filter details	
Interface name filter	Using regular expression, provide the name of the interface for the devices you want to monitor or the devices you do not want to monitor. **Examples** ◆ To monitor all interfaces, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude interface name filter.* ◆ To monitor all interfaces, enter `"*"` and select **Include** in *Include or exclude interface name filter.* ◆ To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude interface name filter.* ◆ To monitor only ethernet interfaces, enter `(?=Ethernet)` and select **Include** in *Include or exclude interface name filter.* ◆ To monitor all interfaces EXCEPT ethernet interfaces, enter `(?=Ethernet)` and select **Exclude** in *Include or exclude interface name filter.*
Include or exclude interface name filter	Select **Include** to monitor only the devices for the interfaces you specified in *Interface name filter*. Select **Exclude** to monitor all devices except for those associated with the interfaces you specified in *Interface name filter.*
Collect data for operational interfaces and total interfaces?	Select **Yes** to collect data about the number of interfaces that are operational and the total number of interfaces for use in charts and reports. The default is No.
Event severity when interface goes down	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface's operational status changes from Up to Down. Enter **0** if you do not want to raise an event. The default is 5. By default, this script raises one event only when the operational status changes to Down. If you want to raise an event every time the Knowledge Script runs to indicate that the interface is *still* down, use the *Raise the "Interface down" event on every job iteration* parameter.
Event severity when interface comes up	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface's operational status changes from Down to Up. Enter **0** if you do not want to raise an event. The default is 25.

Parameter	How to Set It
Event severity when interface goes administratively down	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface's administrative status changes from Up to Down. The default is 15. By default, this script raises one event only when the administrative status changes to Down. If you want to raise an event every time the Knowledge Script runs to indicate that the interface is *still* down, use the *Raise the "Interface down" event on every job iteration* parameter.
Event severity when interface comes administratively and operationally back up	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface's administrative *and* operational statuses change from Down to Up. The default is 30.
Raise the "Interface down" event on every job iteration	Select **Yes** to raise an event for each job iteration in which an interface's operational or administrative status is Down. To raise one event only when the status changes from Up to Down, set this parameter to No. The default is No.
Ignore the administratively down interfaces	Select **Yes** to prevent AppManager from raising an event when an interface is down for administrative purposes. Accept the default of **No** if you want AppManager to raise an event when an interface is down for administrative purposes.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.20 IPSubsystem_Util

Use this Knowledge Script to monitor the IP subsystem of a network device, including inbound and outbound packet rates and packet error rates. This script raises an event if the packet error rate exceeds the threshold you set. In addition, this script generates datastreams for packet error rates and the number of packet errors.

Resource Object

NetworkDevice IP Subsystem

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the IPSubsystem_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Collect data for packet rate and packet errors?	Select **Yes** to collect data about packet rates and packet errors for charts and graphs. The default is No.
Threshold - Maximum packet error rate	Specify the maximum packet error rate that can occur before an event is raised. The default is 8%.
Event severity when packet error rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the packet error rate exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive packet error rate. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to No.

3.21 ISDNChannel_CallVolume

Use this Knowledge Script to measure the number of incoming calls, the number of outgoing calls, and the percentage of call failures (dropped calls) on a device. This script raises an event if the dropped call rate exceeds the threshold you set. In addition, this script generates datastreams for incoming and outgoing call rates and dropped calls.

Resource Object

NetworkDevice ISDN Channel Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the ISDNChannel_CallVolume job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Filter Details	
Channel name filter	Using regular expression, specify the names of the channels you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude channel name filter* parameter. **Examples** ◆ To monitor all channels, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude channel name filter.* ◆ To monitor all channels, enter `"*"` and select **Include** in *Include or exclude channel name filter.* ◆ To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude channel name filter.*
Include or exclude channel name filter	Select **Include** to monitor only the channels you specified in *Channel name filter*. Select **Exclude** to monitor all channels except those you specified in *Channel name filter.*
Collect data for call rate and dropped calls?	Select **Yes** to collect data about incoming call rates, outgoing call rates, and percentage of dropped calls for charts and graphs.
Threshold - Maximum dropped call rate	Specify the maximum percentage of dropped (failed) calls that can occur before an event is raised.

Parameter	How to Set It
Event severity when dropped call rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of dropped calls exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to No.

3.22 ISDNChannel_Health

Use this Knowledge Script to monitor the operational status of ISDN bearer channels and the up-or-down status of signaling channels. This script raises an event if the percentage of operational ISDN bearer channels falls below the threshold that you set or if a signaling channel is down. In addition, this script generates datastreams for operational ISDN bearer channels (as a percentage of all bearer channels) and signaling channel status.

Resource Object

NetworkDevice ISDN Channel Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the ISDNChannel_Health job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.

Parameter	How to Set It
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Filter Details	
Channel name filter	Using regular expression, specify the names of the channels you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude channel name filter* parameter. **Examples** ◆ To monitor all channels, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude channel name filter.* ◆ To monitor all channels, enter "*" and select **Include** in *Include or exclude channel name filter.* ◆ To monitor nothing, enter "*" and select **Exclude** in *Include or exclude channel name filter.*
Include or exclude channel name filter	Select **Include** to monitor only the channels you specified in *Channel name filter*. Select **Exclude** to monitor all channels except those you specified in *Channel name filter.*
Collect data for operational bearer channels?	Select **Yes** to collect data for charts and graphs. If enabled, data collection returns the percentage of bearer channels that were operational during the monitoring period. The default is Yes.
Threshold - Minimum operational bearer channels	Specify the minimum percentage of channels that must be operational to prevent an event from being raised. The default is 99%.
Event severity when operational bearer channels fall below threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the number of operational channels falls below the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Collect data for ISDN signaling channel status?	Select **Yes** to collect data for charts and graphs. If enabled, data collection returns 100 if the signaling channel is up and 0 if the signaling channel is down. The default is Yes.
Event severity when the ISDN signaling channel is down	Set the severity level, between 1 and 40, to indicate the importance of an event in which the signaling channel is down. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to No.

3.23 ISDNChannel_Util

Use this Knowledge Script to measure the usage of ISDN channels on a device. This script raises an event if channel usage exceeds the specified threshold. In addition, this script generates datastreams for ISDN channel usage.

Resource Object

NetworkDevice ISDN Channel Folder

Default Schedule

By default, this script runs every minute.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the ISDNChannel_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Filter Details	

Parameter	How to Set It
Channel name filter	Using regular expression, specify the names of the channels you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude channel name filter* parameter. **Examples** ◆ To monitor all channels, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude channel name filter.* ◆ To monitor all channels, enter "*" and select **Include** in *Include or exclude channel name filter.* ◆ To monitor nothing, enter "*" and select **Exclude** in *Include or exclude channel name filter.*
Include or exclude channel name filter	Select **Include** to monitor only the channels you specified in *Channel name filter*. Select **Exclude** to monitor all channels except those you specified in *Channel name filter.*
Collect data for ISDN channel utilization?	Select **Yes** to collect data about channel usage for charts and graphs. The default is Yes.
Threshold - Maximum ISDN channel utilization	Specify the maximum percentage of channel usage that can occur before an event is raised. The default is 80%.
Event severity when ISDN channel utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of channel usage exceeds the threshold that you set. The default is 10. Set the severity level to **0** if you do not want to raise an event.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to No.

3.24 LANLink_QoS

Use this Knowledge Script to monitor Quality of Service (QoS) on LAN links on a Cisco IOS device. This script monitors traffic class usage, dropped packet rate, and queue depth. This script raises an event if a monitored value exceeds the threshold you set.

Traffic class

A particular category of traffic on an interface. For example, voice and data can be classified as individual traffic classes.

Queue

The virtual buffer associated with a particular traffic class.

Dropped packet rate

The rate at which packets are dropped because of factors such as queuing, policing, early detection, or traffic shaping.

Queue depth

The number of packets in a queue.

Policy

The action that QoS takes within a traffic class upon the traffic that enters the class, such as dropping packets. Pre-policy traffic is the traffic that flows into a traffic class, before QoS applies a policy. Post-policy is the traffic that leaves a traffic class after a policy has been applied.

Resource Object

NetworkDevice LAN Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the LANLink_QoS job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.

Parameter	How to Set It
Link name filter	Using regular expression, specify the names of the LAN links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** ◆ To monitor all LAN links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* ◆ To monitor all LAN links, enter `"*"` and select **Include** in *Include or exclude link name filter.* ◆ To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter.* ◆ To monitor only ip links, enter `(?=ip)` and select **Include** in *Include or exclude link name filter.* ◆ To monitor all interfaces EXCEPT ip links, enter `(?=ip)` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the LAN links you specified in *Link name filter*. Select **Exclude** to monitor all LAN links except those you specified in *Link name filter.*
Class name filter	Using regular expression, specify the name of the traffic classes that you want to monitor. Leave this parameter blank to monitor all traffic classes.
Traffic Class Utilization	
Monitor traffic class utilization?	Select **Yes** to monitor traffic class usage and to activate the parameters in this section. The default is Yes.
Collect data for traffic class utilization?	Select **Yes** to collect data for charts and graphs. This script generates datastreams for the pre-policy and post-policy bandwidth used by each configured traffic class. The default is No.
Threshold - Maximum traffic class utilization	Specify the maximum percentage of traffic class usage that can occur before an event is raised. The default is 25%.
Event severity when traffic class utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of traffic class usage exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Collect data for traffic class pre/post policy bytes?	Select **Yes** to collect data for charts and graphs. The default is No. This script generates datastreams for the number of pre- and post-policy bytes per second.
Select unit for traffic class pre/post policy bytes	Select the unit for collecting data for the pre/post policy bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Queue Depth	
Monitor queue depth?	Select **Yes** to monitor the queue depth. The default is Yes.
Collect data for queue depth?	Select **Yes** to collect data for charts and graphs. The default is No. This script generates datastreams for queue depth (number of packets) by class name.

Parameter	How to Set It
Threshold - Maximum priority queue depth	Specify the highest number of packets that a priority queue can contain before an event is raised. The default is 0 packets.
Threshold - Maximum non-priority queue depth	Specify the highest number of packets that a non-priority queue can contain before an event is raised. The default is 10 packets.
Event severity when queue depth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the queue depth exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Dropped Packets	
Monitor dropped packet rate?	Select **Yes** to monitor the rate at which packets are dropped from the traffic class and to activate the parameters in this section. The default is Yes.
Collect data for dropped packet rate?	Select **Yes** to collect data for charts and graphs. The default is No. This script generates datastreams for the percentage of dropped packets, and for the number of packets dropped per second.
Threshold - Maximum dropped packet rate	Specify the maximum rate at which packets can be dropped from the traffic class before an event is raised. The default is 1%.
Event severity when dropped packet rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the dropped packet rate exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to No.

3.25 LANLink_Util

Use this Knowledge Script to monitor the parent resource for the Local Area Network (LAN) links on a network device. This script creates datastreams for bandwidth usage, inbound and outbound packet rates, and inbound and outbound packet error rates. This script raises an event if a monitored value exceeds the threshold you set. In addition, this script generates datastreams for bandwidth usage and link errors.

NOTE: LANLink_Util differs from SingleLANLink_Util in that it lets you monitor all links for all devices of any parent resource. SingleLANLink_Util allows you to monitor selected links for only one device.

Resource Object

NetworkDevice LAN Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the LANLink_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Link name filter	Using regular expressions, specify the names of the LAN links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** ◆ To monitor all LAN links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* ◆ To monitor all LAN links, enter `"*"` and select **Include** in *Include or exclude link name filter.* ◆ To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter.* ◆ To monitor only ip links, enter `(?=ip)` and select **Include** in *Include or exclude link name filter.* ◆ To monitor all interfaces EXCEPT ip links, enter `(?=ip)` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the LAN links you specified in *Link name filter*. Select **Exclude** to monitor all LAN links except those you specified in *Link name filter.*
Link Utilization	

Parameter	How to Set It
Monitor link utilization?	Select **Yes** to monitor link usage and to activate the parameters in this section. The default is Yes.
Collect data for bandwidth utilization?	Select **Yes** to collect data about bandwidth usage for charts and graphs. The default is Yes.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Select **Yes** to collect data about sent and received bytes for charts and graphs. The default is No.
Select unit for bytes sent/received	Select the unit for collecting data for the sent/received bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Collect data for inbound/outbound bandwidth utilization?	Select **Yes** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is No.
Link Errors	
Monitor link errors?	Select **Yes** to monitor link errors and to activate the parameters in this section. The default is Yes.
Collect data for link errors?	Select **Yes** to collect data about link errors for charts and graphs. The default is No.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 8%.
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Include discards in link errors?	Select **Yes** to include discarded incoming packets in the packet error calculation. The default is Yes. If set to Yes, the calculation for packet errors is as follows: `(notdeliveredpackets/deliveredpackets)*100%/time elapsed` where *delivered packets* = sum(UCastPkts, NUCastPkts) and *not delivered packets* = sum(errors, discards, unknown protocols) Errors are defined as packet errors. Unknown protocols are unsupported protocols. Discards are packets discarded for any other reason.

Parameter	How to Set It
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.26 Report_DeviceAvailability

Use this Knowledge Script to summarize the availability of selected network devices over a specified time period. This script uses the data collected by the Device_Ping Knowledge Script.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select devices for report	Select the network devices whose data you want to include in your report.
Select Knowledge Script	Specify the name of the Knowledge Script to include in your report. Specify one script per report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Report Settings	
Decimal accuracy for % values	Specify the number of decimal places that you want to see in the percentage values generated by this report. The default is 3.
Include parameter card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include charts?	Select **Yes** to include charts of datastream values in the report. The default is Yes.

Parameter	How to Set It
Include tables?	Select **Yes** to include a table of datastream values in the report. The default is Yes.
Select chart style	Define the graphic properties of the charts in your report. The default chart style is Line.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceAvailability.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is No. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Set the report properties as desired. The default report name is Network Device Availability.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The default is No. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

3.27 Report_ChassisUsage

Use this Knowledge Script to summarize the Good-Acceptable-Poor (GAP) ratings and average usage for CPU, memory pool, and backplane for a network device. This script uses the data collected by the Chassis_Usage Knowledge Script.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select Knowledge Scripts	Select the Knowledge Scripts to include in your report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekdays	Select the days of the week to include in your report. The default is every day of the week.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Chart Thresholds	
Good-Acceptable CPU utilization threshold	Specify the Good-Acceptable CPU usage threshold to display on the charts in the report. The default is 30%.
Acceptable-Poor CPU utilization threshold	Specify the Acceptable-Poor CPU usage threshold to display on the charts in the report. The default is 50%.
Good-Acceptable memory pool utilization threshold	Specify the Good-Acceptable memory pool usage threshold to display on the charts in the report. The default is 30%.
Acceptable-Poor memory pool utilization threshold	Specify the Acceptable-Poor memory pool usage threshold to display on the charts in the report. The default is 50%.
Good-Acceptable backplane utilization threshold	Specify the Good-Acceptable backplane usage threshold to display on the charts in the report. The default is 50%.
Acceptable-Poor backplane utilization threshold	Specify the Acceptable-Poor backplane usage threshold to display on the charts in the report. The default is 75%.
Report Settings	
Include parameter card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include charts?	Select **Yes** to include charts of datastream values in the report. The default is Yes.
Include tables?	Select **Yes** to include tables of datastream values in the report. The default is Yes.
Select Average Utilization chart properties	Set chart properties, such as style, thresholds, and size. The default style is Area.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceChassisUsage.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is No. The job ID helps you correlate a specific instance of a Report script with the corresponding report.

Parameter	How to Set It
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device Chassis Usage Summary.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The default is No. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

3.28 Report_ISDNCallVolume

Use this Knowledge Script to summarize the average ISDN channel call volume for the links on selected devices over a time range. This Knowledge Script uses data collected by the ISDNChannel_CallVolume Knowledge Script.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select granularity filter	Select **Trunk** or **Gateway** to determine the granularity of data gathered for your report. Selecting **Trunk** generates one chart per gateway, while selecting **Gateway** generates a single chart displaying data for each gateway. The default is Trunk.

Parameter	How to Set It
Select Knowledge Scripts	Select the Knowledge Scripts to include in your report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Chart Thresholds	
Call volume threshold	Specify the call volume threshold to display on the charts in the report. Accept the default of **0** if you do not want to display this threshold.
Dropped call threshold	Specify the dropped call threshold to display on the charts in the report. Accept the default of **0** if you do not want to display this threshold.
Report Settings	
Include parameter card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include charts?	Select **Yes** to include charts of datastream values in the report. The default is Yes.
Include tables?	Select **Yes** to include tables of datastream values in the report. The default is Yes.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceISDNChannelCallVolume.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is No. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device ISDN Channel Call Volume Summary.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The default is No. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

3.29 Report_ISDNTimeDetail

Use this Knowledge Script to summarize the average ISDN statistics on selected trunks over a time range. This script uses data collected by the ISDNChannel_Util and ISDNChannel_CallVolume Knowledge Scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select link(s) for report	Select the links whose data you want to include in your report.
Select Knowledge Scripts	Select the Knowledge Scripts to include in your report.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Include parameter card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include charts?	Select **Yes** to include charts of datastream values in the report. The default is Yes.
Include tables?	Select **Yes** to include tables of datastream values in the report. The default is Yes.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceISDNTimeDetail.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is No. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device ISDN Time Detail Summary.

Parameter	How to Set It
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The default is No. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

3.30 Report_ISDNUtilization

Use this Knowledge Script to summarize the average ISDN channel call volume for the trunks on selected devices over a time range. This script uses the data collected by the ISDNChannel_CallVolume Knowledge Script.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select granularity filter	Select **Trunk** or **Gateway** to determine the granularity of data gathered for your report. Selecting **Trunk** generates one chart per gateway, while selecting **Gateway** generates a single chart displaying data for each gateway. The default is Trunk.
Select Knowledge Scripts	Select the Knowledge Scripts to include in your report.

Parameter	How to Set It
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Chart Thresholds	
Good-Acceptable channel utilization threshold	Specify the Good-Acceptable channel usage threshold to display on the charts in the report. The default is 30%.
Acceptable-Poor channel utilization threshold	Specify the Acceptable-Poor channel usage threshold to display on the charts in the report. The default is 50%.
Channel utilization threshold	Specify the channel usage threshold to display on the charts in the report. Accept the default of 0% if you do not want to display this threshold.
Channel Utilization Chart Settings	
Select chart properties	Set chart properties, such as style, thresholds, and size. The default chart style is Bar.
Report Settings	
Include parameter card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include charts?	Select **Yes** to include charts of datastream values in the report. The default is Yes.
Include tables?	Select **Yes** to include a table of datastream values in the report. The default is Yes.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceISDNChannelUtilization.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is No. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device ISDN Channel Utilization Summary.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The default is No. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.

Parameter	How to Set It
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

3.31 Report_LinkUtilization

Use this Knowledge Script to summarize average link usage within a specified time frame. This script uses the data collected by the link usage Knowledge Scripts.

NOTE: The Report_LinkUtilization Knowledge Script displays the datastream values on charts in megabytes per second irrespective of the units you select in the different _Util Knowledge Scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select Knowledge Script	Select the Knowledge Script to include in your report. Select one script per report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Chart Thresholds	
Good-Acceptable bandwidth utilization threshold	Specify the Good-Acceptable bandwidth usage threshold to display on the charts in the report. The default is 30%.
Acceptable-Poor bandwidth utilization threshold	Specify the Acceptable-Poor bandwidth usage threshold to display on the charts in the report. The default is 50%.
Total volume threshold	Specify the volume threshold to display on the charts in the report. Enter **0** if you do not want to display a threshold. The default is 0 megabytes/second.

Parameter	How to Set It
Packet Errors Chart Settings	
Select chart properties	Set chart properties, such as style, thresholds, and size. The default chart style is Bar.
Report Settings	
Include parameter card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include charts?	Select **Yes** to include charts of datastream values in the report. The default is Yes.
Include tables?	Select **Yes** to include tables of datastream values in the report. The default is Yes.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceLinkUtilization.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is No. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device Link Utilization.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is No.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

3.32 Report_QoSUtilization

Use this Knowledge Script to summarize average traffic class statistics for the links on selected devices over a time range. This script uses data collected by the link QoS Knowledge Scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select datastream type	Select the type of datastream to include in your report. The default is Post-policy bandwidth. **NOTE:** For Pre-policy bytes and Post-policy bytes, this report Knowledge Script displays the datastream values on charts in megabytes/second irrespective of the units you select in the different _QoS Knowledge Scripts.
Select Knowledge Script	Specify the name of the Knowledge Script to include in your report. Specify one script per report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Include parameter card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include charts?	Select **Yes** to include charts of datastream values in the report. The default is Yes.
Include tables?	Select **Yes** to include tables of datastream values in the report. The default is Yes.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceQoSUtilization.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is No. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device QoS Utilization Summary.

Parameter	How to Set It
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is No.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

3.33 Report_QoSVolume

Use this Knowledge Script to summarize average traffic class statistics for the links on selected devices over a time range. This Knowledge Script uses data collected by the link QoS Knowledge Scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select link(s) for report	Select the network devices whose data you want to include in your report.

Parameter	How to Set It
Select datastream type	Select the type of datastream to include in your report. The default is Post-policy bandwidth. **NOTE:** For Pre-policy bytes and Post-policy bytes, this report Knowledge Script displays the datastream values on charts in megabytes/second irrespective of the units you select in the different _QoS Knowledge Scripts.
Select Knowledge Script	Specify the name of the Knowledge Script to include in your report. Specify one Knowledge Script per report.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Include parameter card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include charts?	Select **Yes** to include charts of datastream values in the report. The default is Yes.
Include tables?	Select **Yes** to include tables of datastream values in the report. The default is Yes.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceQoSVolume.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is No. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device QoS Volume Summary.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is No.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

3.34 Report_TotalVolume

Use this Knowledge Script to summarize total volume for selected devices within a specified time frame. This Knowledge Script uses the data collected by the link usage Knowledge Scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

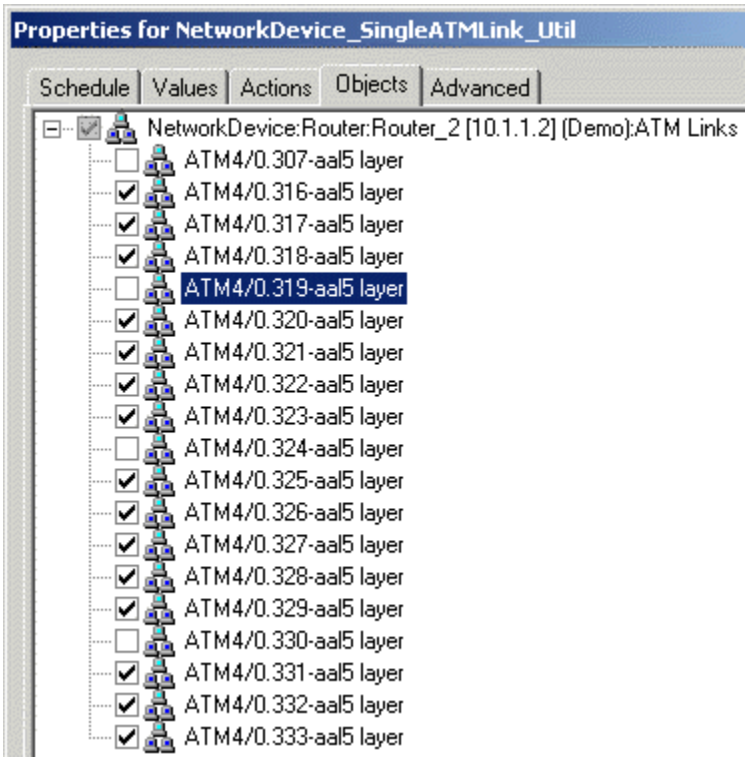
Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select Knowledge Script	Provide the name of the Knowledge Script to include in your report. Specify one script per report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Chart Settings	
Chart size	Select the size of the rendered chart. Choose from **Large**, **Medium**, and **Small**. The default is Medium.
Horizontal chart?	Select **Yes** to include a horizontal chart in your report. The default is No.
Chart color scheme	Select a color scheme template. The default template is NetIQ1.
Chart threshold value	Specify the threshold to be shown on reports. The default is 0 bytes/sec.
Report Settings	
Include parameter card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include charts?	Select **Yes** to include charts of datastream values in the report. The default is Yes.
Include tables?	Select **Yes** to include tables of datastream values in the report. The default is Yes.

Parameter	How to Set It
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceTotalVolume.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is No. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device Total Volume.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is No.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

3.35 SingleATMLink_Util

Use this Knowledge Script to monitor the usage of the Asynchronous Transfer Mode (ATM) links on a single network device. This script raises an event if any value exceeds a specified threshold. In addition, this script generates datastreams for bandwidth usage, packet rate, and packet error rate.

SingleATMLink_Util differs from ATMLink_Util in that it allows you to choose the link you want to monitor for a single device. Click the Objects tab and select the appropriate links.



Resource Object

NetworkDevice

If you run the script on a large number of objects (roughly 100 or more), the Operator Console or Control Center console may take up to 30 seconds to display the Properties dialog box for the Knowledge Script. In addition, 100% of system CPU may be consumed during this 30-second period.

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
General Settings	

Description	How to Set It
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SingleATMLink_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Link Utilization	
Monitor link utilization?	Select **Yes** to monitor link usage and to activate the parameters in this section. The default is Yes.
Collect data for bandwidth utilization?	Select **Yes** to collect data about bandwidth usage for charts and graphs. The default is Yes.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Select **Yes** to collect data about sent and received bytes for charts and graphs. The default is Yes.
Select unit for bytes sent/received	Select the unit for collecting data for the sent/received bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Collect data for inbound/outbound bandwidth utilization?	Select **Yes** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is No.
Link Errors	
Monitor link errors?	Select **Yes** to monitor link errors and to activate the parameters in this section. The default is Yes.
Collect data for link errors?	Select **Yes** to collect data about link errors for charts and graphs. The default is Yes.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 8%.

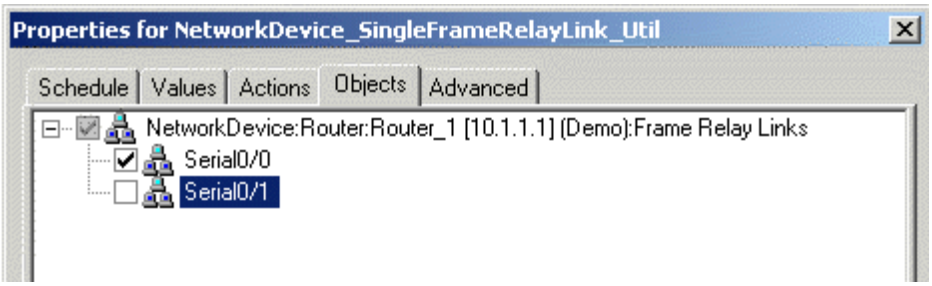
Description	How to Set It
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to No.

3.36 SingleFrameRelayLink_Util

Use this Knowledge Script to monitor the usage of the frame relay links on a single network device. A frame relay link uses a packet-switching protocol for connecting devices on a Wide Area Network (WAN). This script raises an event if any value exceeds a specified threshold. In addition, this script generates datastreams for the following:

- Bandwidth usage
- Frame rate
- FECN (Forward Explicit Congestion Notification) rate. A *FECN* is a frame relay message that notifies the receiving device that there is congestion in the network. A FECN bit is sent in the direction in which the frame is traveling, toward its destination.
- BECN (Backward Explicit Congestion Notification) rate. A *BECN* is a frame relay message that notifies the sending device that there is congestion in the network. A BECN bit is sent in the direction from which the frame is traveling, toward its transmission source.

SingleFrameRelayLink_Util differs from FrameRelayLink_Util in that it allows you to choose which links you want to monitor for a single device. On the Objects tab, select the appropriate links. For example:



Resource Object

NetworkDevice

If you run the script on a large number of objects (roughly 100 or more), the Operator Console may take up to 30 seconds to display the Properties dialog box. In addition, 100% of system CPU may be consumed during this 30-second period.

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SingleFrameRelayLink_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Link Utilization	
Monitor link utilization?	Select **Yes** to monitor link usage and to activate the parameters in this section. The default is Yes.
Collect data for bandwidth utilization?	Select **Yes** to collect data about bandwidth usage for charts and graphs. The default is Yes.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Select **Yes** to collect data about sent and received bytes for charts and graphs. The default is Yes.
Select unit for bytes sent/received	Select the unit for collecting data for the sent/received bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Collect data for inbound/outbound bandwidth utilization?	Select **Yes** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is No.
Link Errors	

Parameter	How to Set It
Monitor FECNs/BECNs?	Select **Yes** to monitor FECN and BECN rates and to activate the parameters in this section. The default is Yes.
Collect data for FECNs/BECNs?	Select **Yes** to collect data about FECN and BECN rates for charts and graphs. The default is Yes.
Threshold - Maximum FECNs/BECNs	Specify the maximum percentage of FECN/BECN rates that can occur before an event is raised. The default is 8%.
Event severity when FECNs/BECNs exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of FECN/BECN rates exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.37 SingleInterface_Health

Use this Knowledge Script to monitor the interfaces on a single network device. This script raises an event if the interface status changes or if any value exceeds a specified threshold. In addition, this script generates a datastream indicating the up or down status of the interface.

SingleInterface_Health differs from Interface_Health in that it allows you to choose which interface you want to monitor for a single device. On the Objects tab, select the appropriate interfaces. For example:

Resource Object

NetworkDevice

If you run the script on a large number of objects (roughly 100 or more), the Operator Console or Control Center console may take up to 30 seconds to display the Properties dialog box for the Knowledge Script. In addition, 100% of system CPU may be consumed during this 30-second period.

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

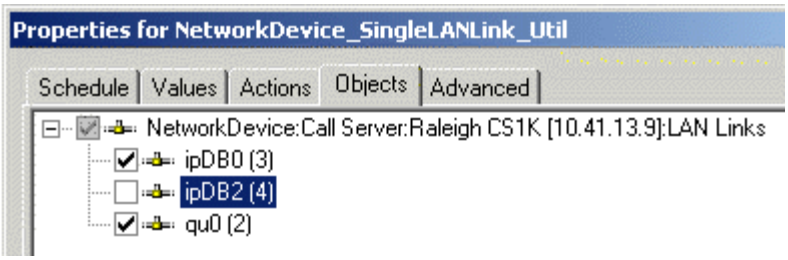
Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SingleInterface_Health job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Collect data for interface status?	Select **Yes** to collect data about interface status for charts and graphs. The default is Yes.
Event severity when interface goes down	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface status changes from Up to Down. Enter **0** if you do not want to raise an event. The default is 5.
Event severity when interface comes back up	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface status changes from Down to Up. Enter **0** if you do not want to raise an event. The default is 15.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.38 SingleLANLink_Util

Use this Knowledge Script to monitor the Local Area Network (LAN) links on a single network device. This script raises an event if a threshold is exceeded. In addition, this script generates datastreams for bandwidth usage, inbound and outbound packet rates, and inbound and outbound packet error rates.

SingleLANLink_Util differs from LANLink_Util in that it allows you to choose which links you want to monitor for a single device. On the Objects tab, select the appropriate links. For example:



Resource Object

NetworkDevice

If you run the script on a large number of objects (roughly 100 or more), the Operator Console or Control Center console may take up to 30 seconds to display the Properties dialog box for the Knowledge Script. In addition, 100% of system CPU may be consumed during this 30-second period.

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SingleLANLink_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.

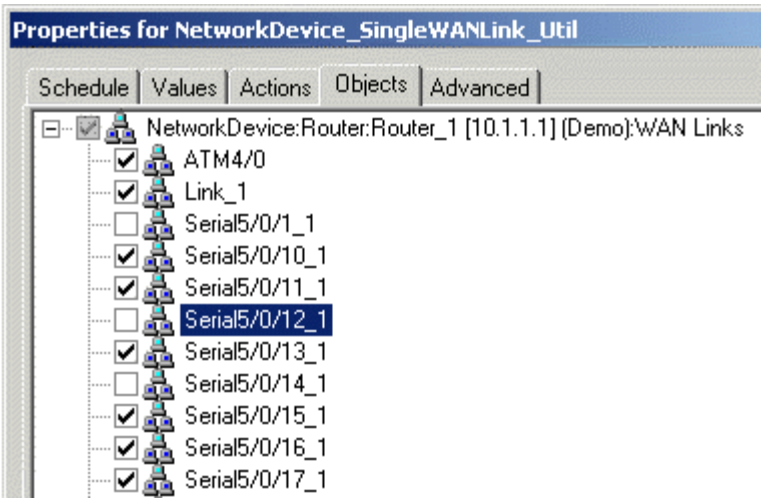
Parameter	How to Set It
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Link Utilization	
Monitor link utilization?	Select **Yes** to monitor link usage and to activate the parameters in this section. The default is Yes.
Collect data for bandwidth utilization?	Select **Yes** to collect data about bandwidth usage for charts and graphs. the default is Yes.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Select **Yes** to collect data about sent and received bytes for charts and graphs. The default is Yes.
Select unit for bytes sent/received	Select the unit for collecting data for the sent/received bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Collect data for inbound/outbound bandwidth utilization?	Select **Yes** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is No.
Link Errors	
Monitor link errors?	Select **Yes** to monitor link errors and to activate the parameters in this section. The default is Yes.
Collect data for link errors?	Select **Yes** to collect data about link errors for charts and graphs. The default is Yes.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 8%.
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.

Parameter	How to Set It
Include discards in link errors?	Select **Yes** to include discarded incoming packets in the packet error calculation. The default is Yes. If set to Yes, the packet error calculation is as follows: `(notdeliveredpackets/deliveredpackets)*100%/time elapsed` where *delivered packets* = sum(UCastPkts, NUCastPkts) and *not delivered packets* = sum(errors, discards, unknown protocols) Errors are defined as packet errors. Unknown protocols are unsupported protocols. Discards are packets discarded for any other reason.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to No.

3.39 SingleWANLink_Util

Use this Knowledge Script to monitor the serial, T1, or T3 links on a single network device. This script raises an event if any value exceeds a threshold you set. In addition, this script generates datastreams for bandwidth usage, inbound and outbound packet rates, and inbound and outbound packet error rates.

SingleWANLink_Util differs from WANLink_Util in that it allows you to choose the link you want to monitor for a single device. On the Objects tab, select the appropriate links. For example:



Resource Object

NetworkDevice

If you run the script on a large number of objects (roughly 100 or more), the Operator Console or Control Center console may take up to 30 seconds to display the Properties dialog box for the Knowledge Script. In addition, 100% of system CPU may be consumed during this 30-second period.

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SingleWANLink_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Link Utilization	
Monitor link utilization?	Select **Yes** to monitor link usage and to activate the parameters in this section. The default is Yes.
Collect data for bandwidth utilization?	Select **Yes** to collect data about bandwidth usage for charts and graphs. The default is Yes.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Select **Yes** to collect data about sent and received bytes for charts and graphs. The default is Yes.

Parameter	How to Set It
Select unit for bytes sent/received	Select the unit for collecting data for the sent/received bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Collect data for inbound/outbound bandwidth utilization?	Select **Yes** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is No.
Link Errors	
Monitor link errors?	Select **Yes** to monitor link errors and to activate the parameters in this section. The default is Yes.
Collect data for link errors?	Select **Yes** to collect data about link errors for charts and graphs. The default is Yes.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 8%.
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Include discards in link errors?	Select **Yes** to include discarded incoming packets in the packet error calculation. The default is Yes. If set to Yes, the calculation for packet errors is as follows: `(notdeliveredpackets/deliveredpackets)*100%/time elapsed` where *delivered packets* = sum(UCastPkts, NUCastPkts) and *not delivered packets* = sum(errors, discards, unknown protocols) Errors are defined as packet errors. Unknown protocols are unsupported protocols. Discards are packets discarded for any other reason.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to No.

3.40 SNMPTrap_AddMIB

Use this Knowledge Script to add MIB (management information base) files to the MIB tree that is monitored by the SNMPTrap_Async Knowledge Script. The MIB files should be `ASN.1` text file with a `.txt` or `.my` file extension, and not compiled MIB files.

With this script you can copy a MIB file from an arbitrary directory to the MIB tree located in the `<AppManager directory>\bin\MIBs` directory. And, by using the *Reload MIB tree?* parameter, you can also reload all MIBs in the tree without restarting the AppManager agent. A restart of the AppManager agent automatically reloads the MIB tree.

Scenarios for using this script include the following examples:

In This Scenario	Set These Parameters
You want to add a MIB file to the MIB tree, but do not want the addition to take effect until after the next restart of the AppManager agent.	*Full path to MIB files* and *List of MIB files*: Provide location and name of MIB file you want to add. *Reload MIB tree?*: Select **No** (unselected).
You manually copied a MIB file to the MIB directory and want to reload all MIBs in the directory.	*Full path to MIB files* and *List of MIB files*: Leave blank. *Reload MIB tree?*: Select **Yes**. *MIB reload timeout*: Set new timeout value or accept default of 10 seconds.
Due to compiler errors, you edited some MIBs in the MIB directory. Now you want to reload the MIBs to ensure the errors have been fixed.	*Full path to MIB files* and *List of MIB files*: Leave blank. *Reload MIB tree?*: Select **Yes**. *MIB reload timeout*: Set new timeout value or accept default of 10 seconds.

Resource Object

NetworkDevice Trap Receiver

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Full path to MIB files	Specify the full path to the folder that contains the MIB files you want to install. The AppManager agent on the proxy agent computer must have network access to the location you specify.
List of MIB files	Provide a comma-separated list of the MIB files you want to install. The MIB files should be ASN.1 text files with a `.txt` or `.my` file extension. The MIB files should not be compiled MIB files. The MIB files you specify must be located in the folder you identified in the *Full path to MIB files* parameter.
Reload MIB tree?	Select **Yes** to update the MIB tree.
MIB reload timeout	Specify the length of time AppManager should attempt to update the MIB tree before timing out and raising a failure event. The default is 10 seconds.
Event Notification	

Parameter	How to Set It
Raise event if installation and reloading of MIB tree succeeds?	Select **Yes** to raise an event if installation of the MIB files and/or reloading of the MIB tree succeeds. The default is Yes. Note that reloading of the MIB tree can be successful even if no new MIB files are installed. Reloading of the MIB tree can proceed even if you provide no MIB files in the *List of MIB files* or *Full path to list of MIB files* parameter.
Event severity when installation and reloading of MIB tree succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the installation of MIB files and/or the reloading of the MIB tree succeeds. The default is 25.
Raise event if "reload MIB parser" warnings received?	Select **Yes** to raise an event if warning messages are received during the reload process. The default is Yes. Warning scenarios include: ◆ MIBs are installed successfully but the *Reload MIB tree?* parameter is not set to Yes. ◆ Not all specified MIB files were loaded to the MIB tree.
Event severity when "reload MIB parser" warnings received	Set the severity level, from 1 to 40, to indicate the importance of an event in which warning messages are received during the reload process. The default is 15.
Raise event if installation and reloading of MIB tree fails?	Select **Yes** to raise an event if AppManager fails to install or reload the specified MIB files. The default is Yes. Failure scenarios include: ◆ MIB reload timeout period expired. ◆ Not all specified MIB files were installed.
Event severity when installation and reloading of MIB tree fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the installation or reloading of the MIB tree fails. The default is 10.
Raise event with the list of currently installed MIBs?	Select **Yes** to raise an informational event that provides a list of all MIBs installed in the MIB tree. The default is Yes.
Event severity for list of currently installed MIBs	Set the severity level, from 1 to 40, to indicate the importance of an event that provides a list of all MIBs installed in the MIB tree. The default is 25.

3.41 SNMPTrap_Async

Use this Knowledge Script to check for SNMP traps forwarded from NetIQ SNMP Trap Receiver. This script raises an event when an SNMP trap is received and when Trap Receiver is unavailable or subsequently becomes available. In addition, this script generates datastreams for Trap Receiver availability.

This script checks for SNMP traps in the MIB tree. You can add Management Information Bases (MIBs) to the MIB tree. For more information, see the SNMPTrap_AddMIB Knowledge Script.

In general, a trap receiver is an application that receives traps from SNMP agents. NetIQ SNMP Trap Receiver (Trap Receiver) receives SNMP traps, filters them, and then forwards the traps to AppManager. For more information, see "Working with NetIQ SNMP Trap Receiver" on page 104.

To run this Knowledge Script, you must configure SNMP permissions in Security Manager. For more information, see Section 2.6, “Configuring SNMP Permissions,” on page 17.

Resource Object

NetworkDevice Trap Receiver

Default Schedule

By default, this script runs on an asynchronous schedule.

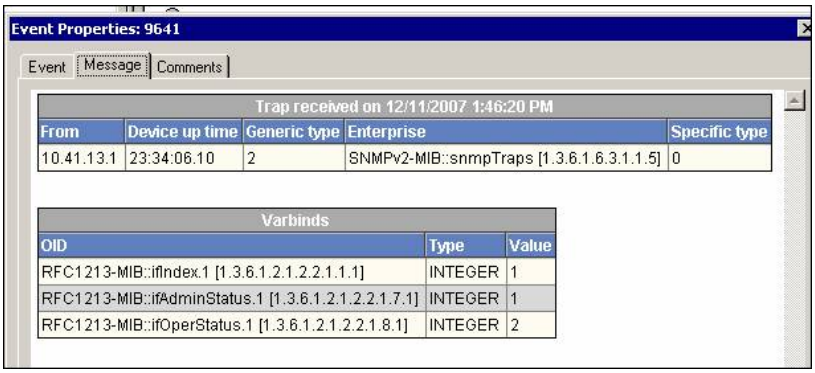
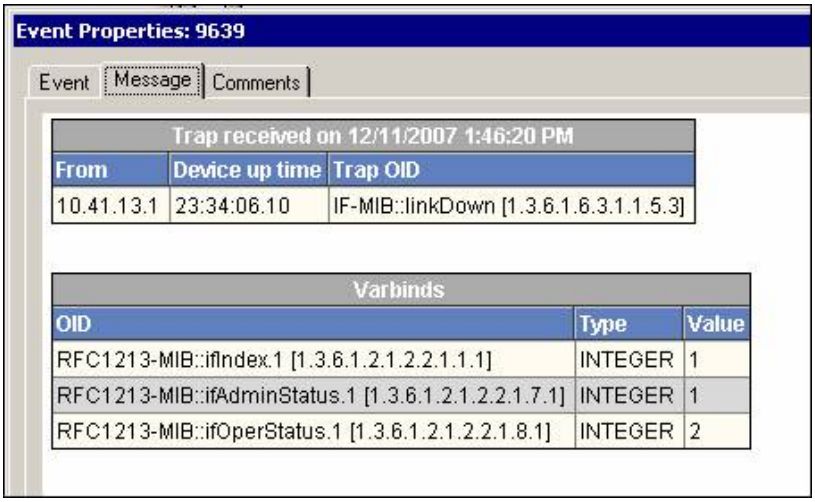
Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Trap Filters	
List of trap OIDs	Specify the OIDs (object identifiers) of the traps you want to monitor. You can type one OID or a list of OIDs. If you type a list, separate the OIDs with a comma. For example: `1.3.6.1.2.1.2.2.1.1.1,1.3.6.1.2.1.2.2.1.7.1`

Full path to file with list of trap OIDs	If you have many OIDs to monitor, you can provide the full path to a file that contains a list of the OIDs. Each OID in the file should be on a separate line. For example:
	
	`1.3.6.1.2.1.2.2.1.1.1`
	`1.3.6.1.2.1.2.2.1.7.1`
	
	Because the file must be accessible from the AppManager agent, the path must be a local directory on the agent computer or a UNC path.
	
	Important For a UNC path, the `netiqmc` service must have permission to access the path.

Event Notification	
Raise trap events?	Select **Yes** to raise an event when a trap message is received from Trap Receiver. The default is Yes.
Event severity when trap is received	Set the severity level, from 1 and 40, to indicate the importance of an event in which a trap is received. The default is 15.

Parameter	How to Set It
Format trap data according to SNMP version	Select the version of SNMP whose formatting should be used for trap event messages. The data provided by each format is the same; only the layout is different. An event message in SNMP v1 format looks like this:  An event message in SNMP v2 format looks like this: 
Raise Trap Receiver availability events?	Select **Yes** to raise an event when Trap Receiver becomes unavailable and when Trap Receiver becomes available once again. The default is Yes.
Event severity when Trap Receiver is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes unavailable. The default is 5.
Event severity when Trap Receiver becomes available	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes available after being unavailable. The default is 25.
Data Collection	
Collect data for Trap Receiver availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns a “1” if Trap Receiver is available and a “0” if Trap Receiver is unavailable. The default is unselected.

Parameter	How to Set It
Interval for collecting Trap Receiver availability data	Specify the frequency with which the script collects Trap Receiver availability data. The default is every 5 minutes.

Working with NetIQ SNMP Trap Receiver

Installation of the AppManager for Network Devices module automatically installs Trap Receiver, which runs as a service: `NetIQTrapReceiver.exe`. Trap Receiver may compete for port usage with any other trap receiver installed on the same computer.

What is NetIQ SNMP Trap Receiver?

At its most basic, a trap receiver is an application that receives traps from SNMP agents. NetIQ SNMP Trap Receiver (Trap Receiver) receives, filters, and forwards SNMP traps to AppManager. When you use Trap Receiver with AppManager for Network Device, the SNMPTrap_Async Knowledge Script raises events when SNMP traps are received.

What is an SNMP Trap?

Simple Network Management Protocol (SNMP) is a protocol-based system used to manage devices on TCP/IP-based networks. From devices on which an SNMP agent resides, such as routers and switches, SNMP sends unsolicited notifications, called traps, to network administrators when thresholds for certain conditions are exceeded. These conditions are defined by the vendor in a device's Management Information Base (MIB); the network administrator sets the thresholds.

Traps are composed of Protocol Data Units (PDUs). Each PDU contains the following information, organized in various ways depending on the version of SNMP in use:

- SNMP version number
- Community name of the SNMP agent
- PDU type
- Enterprise OID (object identifier), a unique number that identifies an enterprise and its system objects in the MIB
- IP address of the SNMP agent
- Generic trap type: Cold start, Warm start, Link down, Link up, Authentication failure, and Enterprise
- Specific trap type. When the Generic trap type is set to "Enterprise," a specific trap type is included in the PDU. A specific trap is unique or specific to an enterprise.
- Time the event occurred
- Varbind (variable binding), a sequence of two fields that contain the OID and a value

Understanding Trap Receiver Architecture

Trap Receiver operates on a Client-Server architecture: the *Server*—the stand-alone Trap Receiver application—receives, filters, and forwards SNMP traps to the *Client*—an application that receives traps, such as AppManager. The Server may receive traps from standard UDP port 162 or from any other configured port. The Client and the Server can reside on the same computer or on separate (proxy) computers.

Communication between Client and Server is implemented as XML messages over a TCP connection. Only one Server is allowed per computer, however, several Clients are allowed per computer. Clients that are registered to the same Server share the same TCP connection. The Server TCP port should be known to all potential Clients.

Understanding the Trap Receiver Configuration File

The configuration file for Trap Receiver, `NetIQTrapReceiver.conf`, identifies the UDP and TCP ports used by Trap Receiver: the UDP port is used for receiving traps; the TCP port is used for communicating with the Client, such as AppManager or another supported NetIQ application. The configuration file also identifies the level of logging you want to use and whether port forwarding is enabled.

By default, the configuration file is installed in `[installation directory]\config`, and has the following format:

```
################################################################
#
# NetIQTrapReceiver.conf
#
# A configuration file for NetIQ SNMP Trap Receiver
#
################################################################
#########################
# TCP port
# Syntax: tcp_port [port]
# E.g. : tcp_port 2735
#########################
tcp_port 2735
#########################
# UDP port
# Syntax: udp_port [port]
# E.g. : udp_port 162
#########################
udp_port 162
#########################
# Forwarding
# Syntax: forward [address]:[port] [v1]
# E.g. : forward 127.0.0.1:1000 v1
#########################
#########################
# Log level
# Syntax: log_level error|warning|info|debug|xml
# E.g. : log_level info
#########################
log_level debug
```

If the configuration file cannot be found, cannot be parsed, or does not contain one of the required values, Trap Receiver is initialized with the default configuration as shown above.

When changing values in the configuration file, take into account the following:

- If you change the TCP port number, stop all asynchronous Knowledge Script jobs associated with the modules that support Trap Receiver. Run the Discovery Knowledge Script on all monitored devices to enable the devices to recognize the new TCP port number.

- If you change the UDP port number, also change the UDP port number configured on the devices that send traps to Trap Receiver.
- If another service uses port 2735 or port 162, Trap Receiver *will not start*. The Trap Receiver log file will contain different levels of messages, based on the log_level you choose. Either change the port numbers in the configuration file, stop the service that is using the default Trap Receiver port numbers, or forward the traps coming in to UDP port 162.
- To forward incoming traps to another trap receiver, such as Microsoft SNMP Trap Service, set the Forwarding values as follows:
  `forward [`*IP address of other trap receiver*`]:[`*port number of other trap receiver*`] [`*SNMP version*`]`.
  For example: `forward 10.40.40.25:167 v1`. By default, incoming traps are not forwarded. For more information, see "Coexisting with Microsoft SNMP Trap Service" on page 106.
- Restart Trap Receiver after any change to the configuration file. From Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **NetIQ Trap Receiver** and select **Restart**.

Coexisting with Microsoft SNMP Trap Service

Two trap receivers cannot be in use on the same computer while using the same standard UDP port (162). If NetIQ SNMP Trap Receiver and another trap receiver such as Microsoft SNMP Trap Service are installed on the same computer and both are receiving traps, then configure Trap Receiver to use the standard UDP port and to forward incoming traps (UDP forwarding) to the other trap receiver. For more information, see "Understanding the Trap Receiver Configuration File" on page 105.

Then, configure the other trap receiver to use a different, non-standard, UDP port that is not in use by another application. The following are instructions for configuring Microsoft SNMP Trap Service.

To configure Microsoft SNMP Trap Service to use another port:

1. Navigate to `c:\Windows\system32\drivers\etc`.
2. Open the **services** file.
3. In the row for `snmptrap`, change the value for **udp** from 162 to another port number that is not in use by any other application. Use the same port number you set as the forwarding port in the Trap Receiver configuration file.
4. Save and close the **services** file.
5. Restart Windows SNMP Trap Service. In Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **SNMP Trap Service** and select **Restart**.

TIP: To see which ports are in use, run `netstat.exe` from a command prompt. Then select an available port as the port for the other trap receiver service.

3.42 WANLink_QoS

Use this Knowledge Script to monitor Quality of Service (QoS) on WAN links on a Cisco IOS device. This script monitors traffic class usage, dropped packet rate, and queue depth. This script raises an event if a monitored value exceeds the threshold you set.

Traffic class

A particular category of traffic on an interface. For example, voice and data can be classified as individual traffic classes.

Queue

The virtual buffer associated with a particular traffic class.

Dropped packet rate

The rate at which packets are dropped because of factors such as queuing, policing, early detection, or traffic shaping.

Queue depth

The number of packets in a queue.

Policy

The action that QoS takes within a traffic class upon the traffic that enters the class, such as dropping packets. Pre-policy traffic is the traffic that flows into a traffic class, before QoS applies a policy. Post-policy is the traffic that leaves a traffic class after a policy has been applied.

Resource Object

NetworkDevice

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the WANLink_QoS job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.

Parameter	How to Set It
Link name filter	Using regular expression, specify the names of the WAN links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** ◆ To monitor all WAN links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* ◆ To monitor all WAN links, enter `"*"` and select **Include** in *Include or exclude link name filter.* ◆ To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter* ◆ To monitor only serial links, enter `(?=serial)` and select **Include** in *Include or exclude link name filter.* ◆ To monitor all interfaces EXCEPT serial links, enter `(?=serial)` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the WAN links you specified in *Link name filter*. Select **Exclude** to monitor all WAN links except those you specified in *Link name filter.*
Class name filter	Using regular expression, specify the name of the traffic classes that you want to monitor. Leave this parameter blank to monitor all traffic classes.
Traffic Class Utilization	
Monitor traffic class utilization?	Select **Yes** to monitor traffic class usage and to activate the parameters in this section. The default is Yes.
Collect data for traffic class utilization?	Select **Yes** to collect data for charts and graphs. The default is No. This script generates datastreams for the pre-policy and post-policy bandwidth used by each configured traffic class.
Threshold - Maximum traffic class utilization	Specify the maximum percentage of traffic class usage that can occur before an event is raised. The default is 25%.
Event severity when traffic class utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of traffic class usage exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Collect data for traffic class pre/post policy bytes?	Select **Yes** to collect data for charts and graphs. This script generates datastreams for the number of pre- and post-policy bytes per second. The default is No.
Select unit for traffic class pre/post policy bytes	Select the unit for collecting data for the pre/post policy bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Queue Depth	
Monitor queue depth?	Select **Yes** to monitor the queue depth. The default is Yes.

Parameter	How to Set It
Collect data for queue depth?	Select **Yes** to collect data for charts and graphs. The default is No. This script generates datastreams for queue depth (number of packets) by class name.
Threshold - Maximum priority queue depth	Specify the maximum number of packets that a priority queue can contain before an event is raised. The default is 0 packets.
Threshold - Maximum non-priority queue depth	Specify the maximum number of packets that a non-priority queue can contain before an event is raised. The default is 10 packets.
Event severity when queue depth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the queue depth exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Dropped Packets	
Monitor dropped packet rate?	Select **Yes** to monitor the rate at which packets are dropped from the traffic class. The default is Yes.
Collect data for dropped packet rate?	Select **Yes** to collect data for charts and graphs. The default is No. This script generates datastreams for the percentage of dropped packets, and for the number of packets dropped per second.
Threshold - Maximum dropped packet rate	Specify the maximum rate at which packets can be dropped from the traffic class before an event is raised. The default is 1%.
Event severity when dropped packet rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the dropped packet rate exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.43 WANLink_Util

Use this Knowledge Script to monitor the parent resource for the serial, T1, or T3 links on a network device. This script raises an event if a monitored value exceeds the threshold you set. In addition, this script generates datastreams for bandwidth usage, inbound and outbound packet rates, and inbound and outbound packet error rates.

NOTE: WANLink_Util differs from SingleWANLink_Utilin that it lets you monitor all links for all devices of any parent resource. SingleWANLink_Util allows you to monitor selected links for only one device.

Resource Object

NetworkDevice WAN Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the WANLink_Util job. The default is 5.
Event severity when job returns warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job completes with warnings. The default is 25.
Event severity when monitoring fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when monitoring fails. The default is 25.
SNMP Settings	
SNMP timeout	Specify the length of time in milliseconds that the job should wait for the SNMP response from the monitored network device before timing out and raising a failure event. The default is 2000 milliseconds.
SNMP retries	Specify the number of times the job should attempt to get the SNMP response from the monitored network device. The default is 1 attempt.
Link name filter	Using regular expression, specify the names of the WAN links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** ◆ To monitor all WAN links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* ◆ To monitor all WAN links, enter `"*"` and select **Include** in *Include or exclude link name filter.* ◆ To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter* ◆ To monitor only serial links, enter `(?=serial)` and select **Include** in *Include or exclude link name filter.* ◆ To monitor all interfaces EXCEPT serial links, enter `(?=serial)` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the WAN links you specified in *Link name filter*. Select **Exclude** to monitor all WAN links except those you specified in *Link name filter.*
Link Utilization	

Parameter	How to Set It
Monitor link utilization?	Select **Yes** to monitor link usage and to activate the parameters in this section. The default is Yes. **Hint** If you set this parameter to **No**, the WANLink_Util job does not raise events for usage and does not generate datastreams. To generate datastreams for usage without raising events, perform the following steps: Set the *Monitor link utilization?* parameter to Yes. Set the *Threshold - Maximum bandwidth utilization* parameter to 100%.
Collect data for bandwidth utilization?	Select **Yes** to collect data about bandwidth usage for charts and graphs. The default is Yes.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Select **Yes** to collect data about sent and received bytes for charts and graphs. The default is Yes.
Select unit for bytes sent/received	Select the unit for collecting data for the sent/received bytes. You can select from bytes per second, kilobytes per second, and megabytes per second. The default is bytes per second.
Collect data for inbound/outbound bandwidth utilization?	Select **Yes** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is No.
Link Errors	
Monitor link errors?	Select **Yes** to monitor link errors and to activate the parameters in this section. The default is Yes.
Collect data for link errors?	Select **Yes** to collect data about link errors for charts and graphs. The default is No.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 8%.
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.

Parameter	How to Set It
Include discards in link errors?	Select **Yes** to include discarded incoming packets in the packet error calculation. The default is Yes. If set to Yes, the packet error calculation is as follows: `(notdeliveredpackets/deliveredpackets)*100%/time elapsed` where *delivered packets* = sum(UCastPkts, NUCastPkts) and *not delivered packets* = sum(errors, discards, unknown protocols) Errors are defined as packet errors. Unknown protocols are unsupported protocols. Discards are packets discarded for any other reason.
Raise one-time events?	Select **Yes** to raise an event for all one-time events. For example, if you set this parameter to Yes, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **No**.

3.44 Recommended Knowledge Scripts

NetIQ Corporation recommends using the following Knowledge Scripts to ensure optimal monitoring of network devices.

- ATMLink_Util
- Chassis_Usage
- Device_Ping
- Device_Uptime
- FrameRelayLink_Util
- FXOPort_Health
- FXOPort_Util
- FXSPort_Health
- FXSPort_Util
- Interface_Health
- IPSubsystem_Util
- LANLink_Util
- WANLink_Util